

Oracle® Communications
PMAC Management and Configuration
Release 6.6.x
Configuration Guide
F17461-01

March 2019

ORACLE®

Oracle Communications PMAC Configuration Guide, Release 6.6.x

Copyright © 2016, 2019 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, then 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.



CAUTION: 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 <https://www.oracle.com/us/support/contact/index.html>.

See more information on MOS in the Appendix G:

Table of Contents

| | |
|--|-----------|
| 1. Introduction | 12 |
| 1.1 References | 12 |
| 1.2 Acronyms..... | 12 |
| 1.3 Terminology | 14 |
| 1.4 How to Use this Document | 14 |
| 2. Acquiring Firmware | 15 |
| 2.1 HP..... | 16 |
| 2.2 Oracle Rack Mount Server | 16 |
| 3. Network Procedures | 16 |
| 3.1 Configure netConfig Repository | 16 |
| 3.2 Aggregation Switch — netConfig Procedures | 34 |
| 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)..... | 34 |
| 3.2.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (RMS System, No PMAC Installed) (netConfig)..... | 42 |
| 3.2.3 Configure Cisco 9372TX-E Aggregation Switches (PMAC Installed) (netConfig) | 51 |
| 3.2.4 Replace a Failed 4948/4948E/4948E-F Switch (PMAC Installed) (netConfig) | 58 |
| 3.2.5 Replace a Failed 4948/4948E/4948E-F Switch (RMS System, No PMAC Installed) (netConfig)..... | 65 |
| 3.2.6 Replace a Failed 9372TX-E Switch (PMAC Installed) (netConfig) | 73 |
| 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) | 78 |
| 3.2.8 Replace a Failed Telco T5C-24GT..... | 81 |
| 3.3 C-Class Enclosure Switch — netConfig Procedures | 87 |
| 3.3.1 Configure Cisco 3020 Switch (netConfig) | 87 |
| 3.3.2 Replace a Failed 3020 Switch (netConfig)..... | 92 |
| 3.3.3 Configure HP 6120XG Switch (netConfig) | 94 |
| 3.3.4 Configure HP 6125G Switch (netConfig) | 99 |
| 3.3.5 Configure HP 6125XLG Switch (netConfig) | 104 |
| 3.3.6 Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch (netConfig)..... | 109 |
| 3.4 Utility Procedures | 112 |
| 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch..... | 112 |
| 3.4.2 Configure SNMP Communities and Trap Servers | 114 |
| 3.4.3 Configure SNMPv3 Security Model and Trap Servers..... | 117 |
| 3.4.4 Configure Access List to only allow specific IP to use SNMPv2 community String | 123 |
| 3.4.5 Configure QoS (DSCP and/or CoS) on HP 6120XG Switches | 127 |
| 3.4.6 Configure Port Mirroring | 129 |
| 3.4.7 SwitchConfig to netConfig Repository Configuration | 132 |
| 3.4.8 Cisco Switch SwitchConfig to netConfig Migration | 143 |
| 3.4.9 HP 6120XG SwitchConfig to netConfig Migration..... | 145 |
| 3.4.10 Configure DSCP Marking Using iptablesADM | 147 |

| | | |
|-----------|---|------------|
| 3.4.11 | Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig) | 148 |
| 3.4.12 | Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig) | 150 |
| 4. | Brocade Switch — SwitchConfig Procedures | 153 |
| 4.1 | Configure Brocade Switches | 153 |
| 4.2 | Upgrade Brocade Switch Firmware | 156 |
| 4.3 | Configure Zones in Brocade Switches | 156 |
| 4.4 | Configure Brocade Switch XNMP Trap Target | 160 |
| 5. | SAN Storage Arrays Procedures | 163 |
| 5.1 | Set IP on Fibre Channel Disk Controllers | 163 |
| 5.2 | Configure Fibre Channel Disk Controllers | 164 |
| 5.3 | Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers | 166 |
| 5.4 | Configure Advanced Settings on P2000 Fibre Channel Disk Controllers | 167 |
| 5.5 | Upgrade Firmware on MSA 2012 fc Disk Controllers | 168 |
| 5.6 | Upgrade Firmware on MSA P2000 Disk Controllers | 169 |
| 5.7 | Replace a Failed Disk in MSA 2012fc Array | 169 |
| 5.8 | Replace a Failed Disk in MSA P2000 Disk Array | 171 |
| 6. | Blade Server Procedures | 174 |
| 6.1 | Upgrade Blade Server Firmware | 174 |
| 6.2 | Confirm/Upgrade Blade Server BIOS Settings | 175 |
| 6.2.1 | BIOS Settings for HP Systems | 175 |
| 6.2.2 | BIOS Settings for Oracle Sun Systems | 178 |
| 6.3 | Configure Blade Server iLO Password for Administrator Account | 180 |
| 6.4 | Access the Server Virtual Serial Port | 182 |
| 6.5 | Configure Syscheck Default Route Ping Test | 183 |
| 6.6 | Prepare a System for Extended Power Outage | 183 |
| 6.7 | Bring Up a System After Extended Power Outage | 184 |
| 7. | C7000 Enclosure Procedures | 184 |
| 7.1 | Configure Initial OA IP | 184 |
| 7.2 | Configure Initial OA Settings Using the Configuration Wizard | 187 |
| 7.3 | Configure OA Security | 194 |
| 7.4 | Upgrade or Downgrade OA Firmware | 195 |
| 7.5 | Store OA Configuration on Management Server | 196 |
| 7.6 | Restore OA Configuration from Management Server | 199 |
| 7.7 | Replace Onboard Administrator | 200 |
| 7.8 | Update IPv4 Address | 203 |
| 7.9 | Update IPv6 Address | 206 |
| 7.10 | Add SNMP Trap Destination on OA | 209 |
| 7.11 | Disable SNMP Trap Destination on OA | 211 |
| 7.12 | Delete SNMP Trap Destination on OA | 211 |

| | |
|---|------------|
| 8. Management Server Procedures | 212 |
| 8.1 IPM Management Server..... | 212 |
| 8.2 Upgrade Management Server Firmware | 213 |
| 8.2.1 Upgrade DL360/DL380 Server Firmware..... | 213 |
| 8.2.2 Upgrade Oracle Rack Mount Server Firmware | 214 |
| 9. PMAC Procedures | 214 |
| 9.1 Install TVOE on the Management Server..... | 217 |
| 9.2 Configure TVOE Network | 217 |
| 9.3 Deploy PMAC Guest | 227 |
| 9.4 Set Up PMAC | 231 |
| 9.5 Configure PMAC Application | 236 |
| 9.6 Add Cabinet and Enclosure to the PMAC System Inventory | 240 |
| 9.7 Edit an Enclosure in the PMAC System Inventory | 243 |
| 9.8 Add ISO Images to the PMAC Image Repository | 245 |
| 9.9 IPM Servers Using PMAC Application | 249 |
| 9.10 Install/Upgrade Applications Using PMAC | 251 |
| 9.11 Patch Applications Using PMAC | 254 |
| 9.12 Install PMAC on Redundant DL360 or DL380 | 257 |
| 9.13 Configure Management Server SNMP Trap Target..... | 260 |
| 9.14 Install and Configure PMAC NetBackup Client | 261 |
| 9.15 Add Rack Mount Server to the PMAC System Inventory | 262 |
| 9.16 Edit Rack Mount Server in the PMAC System Inventory | 265 |
| 9.17 Find and Add a Rack Mount Server to the PMAC System Inventory..... | 267 |
| 9.18 Accept Upgrades Using PMAC | 271 |
| 9.19 Reject Upgrades Using PMAC | 273 |
| 9.20 Accept Patches Using PMAC..... | 275 |
| 9.21 Reject Patches Using PMAC..... | 277 |
| 9.22 Initialize PMAC Application | 279 |
| 9.22.1 Initialize PMAC Application Using CLI | 279 |
| 9.22.2 Initialize PMAC Application Using the GUI..... | 282 |
| 9.23 Configure PMAC Application Guest NetBackup Virtual Disk | 286 |
| 9.24 PMAC Guest Migrate NetBackup Client to New File System | 287 |
| 9.25 Update the TVOE Host SNMP Community String from the GUI..... | 287 |
| 9.26 Configure PMAC Application Guest Isoimages Virtual Disk | 293 |
| 9.27 Certificate Management | 294 |
| 9.27.1 Generate a New Certificate Signing Request | 294 |
| 9.27.2 Update an HTTPS Certificate..... | 296 |
| 9.27.3 Import an HTTPS Certificate | 299 |
| 9.27.4 Delete an HTTPS Certificate | 303 |
| 9.28 Use the PMAC File Management System..... | 304 |
| 9.28.1 Use the PMAC File Management System to Delete Files | 304 |
| 9.28.2 Use the PMAC File Management System to View Files | 306 |
| 9.28.3 Use the PMAC File Management System to Download Files..... | 307 |

- 9.29 Delete ISO Images from the PMAC Image Repository 308
- 9.30 Configure PMAC Domain Name System 310
- 9.31 Set User Authentication on the PMAC 314
- 9.32 Configure the PMAC into an Existing Single Sign-On (SSO) Domain 315
- 9.33 Configure an LDAP Server on the PMAC 319
- 9.34 Transfer Image from PMAC Repository to Other Servers..... 321
- 10. Configure SAN Procedures 323**
 - 10.1 Configure SAN Storage Using PMAC Application 323
 - 10.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation 326
- 11. Virtualization Procedures 327**
 - 11.1 Create Guest Server Using PMAC Application 327
 - 11.2 Delete Guest Server Using PMAC Application 333
 - 11.3 Create Guest Server from Guest Archive Using PMAC Application 334
- 12. General TPD-Based Application Procedures 341**
 - 12.1 Back Up TVOE 341
 - 12.2 Configure NTP on TPD-Based Application 342
 - 12.3 Add SNMP Trap Destination on TPD-Based Application 344
 - 12.4 Delete SNMP Trap Destination on TPD-Based Application 345
 - 12.5 Install the NetBackup Client Application..... 346
 - 12.6 Change SNMP Configuration Settings for iLO2 348
 - 12.7 Change SNMP Configuration Settings for iLO3 and iLO4 350
 - 12.8 Change SNMP Configuration Settings for iLOM 352
 - 12.9 Install NetBackup Client with nbAutoInstall 353
 - 12.10 Install/Upgrade NetBackup Client with platcfg 353
 - 12.11 Create LV and Filesystem for NetBackup Client Software..... 358
 - 12.12 Migrate NetBackup Client to New Filesystem 359
 - 12.13 Create NetBackup Client Config File..... 359
- 13. TVOE Host Procedures 360**
 - 13.1 Enable Virtual Guest Watchdogs as Appropriate for the Application 360
 - 13.2 Configure TVOE NetBackup Client 361
- Appendix A. Using WinSCP 362**
- Appendix B. Install P2000 MSA USB Driver 363**
- Appendix C. Determine which Onboard Administrator is Active 366**
- Appendix D. PMAC Features Configuration..... 367**
 - Appendix D.1 Overview 367
 - Appendix D.2 Enabling Features..... 367
 - Appendix D.3 Editing Roles 367
 - Appendix D.4 Features 367

| | | |
|--------------------|--|------------|
| Appendix D.5 | GUI Usage | 367 |
| Appendix D.6 | CLI Usage | 368 |
| Appendix E. | Access and Exit a Server Console Remotely Using iLO..... | 368 |
| Appendix E.1 | Access a Server Console Remotely | 368 |
| Appendix E.2 | Exit a Guest Console Session on an iLO..... | 369 |
| Appendix F. | Attach an ISO Image to a Server Using iLO or iLOM | 369 |
| Appendix F.1 | Attach an ISO Image to an HP Server Using iLO | 369 |
| Appendix F.2 | Attach an ISO Image to an Oracle Rack Mount Server Using iLOM | 375 |
| Appendix G. | Upgrade Cisco 4948 PROM..... | 378 |
| Appendix H. | Operational Dependencies on Platform Account Passwords | 381 |
| Appendix H.1 | PMAC Credentials for Communication with Other System Components..... | 381 |
| Appendix H.2 | PMAC GUI Account Credentials..... | 383 |
| Appendix H.3 | PMAC Linux User Account Credentials | 384 |
| Appendix H.4 | NetConfig Manager Password..... | 384 |
| Appendix I. | Disable SNMP on the OA | 384 |
| Appendix J. | Downgrade Firmware on a 6125G Switch..... | 386 |
| Appendix K. | Downgrade Firmware on a 6125XLG Switch | 396 |
| Appendix L. | Change Switch Passwords (netConfig) | 406 |
| Appendix M. | Uninstall Symantec NetBackup Client | 408 |
| Appendix N. | Configuring NUMA on pmac-deploy | 414 |
| Appendix O. | Update the PMAC GSOAP Cipher List | 415 |
| Appendix P. | Update the TPD-Provd Cipher List | 420 |
| Appendix Q. | Increase the PMAC NetBackup Filesystem Size | 422 |
| Appendix R. | netConfig Backup Configuration/Restore Configuration/Upgrade Firmware with TPD Cipher Change..... | 429 |
| Appendix S. | Enable SNMPv3 Support on the PMAC..... | 431 |
| Appendix S.1 | Prerequisites | 431 |
| Appendix S.2 | Limitations | 432 |
| Appendix S.3 | Procedural Notes: | 432 |
| Appendix S.4 | Obtaining the IPv6 of a server (guest, blade, or RMS) on the control network of the PMAC | 432 |
| Appendix S.5 | PMAC Procedures for Converting to SNMPv3 | 434 |
| Appendix T. | My Oracle Support (MOS) | 438 |

List of Tables

| | |
|--|-----|
| Table 1. Acronyms | 12 |
| Table 2. Installed Packages and Services for NetBackup Client 7.0, 7.1, 7.5, and 7.7 | 409 |

List of Figures

| | |
|---|----|
| Figure 1. Example of a Procedure Step Used in This Document | 15 |
|---|----|

List of Procedures

| | |
|--|-----|
| Procedure 1. Configure netConfig Repository | 19 |
| Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches | 36 |
| Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches | 44 |
| Procedure 4. Configure Cisco 9372TX-E Aggregation Switches | 53 |
| Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch | 59 |
| Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch | 66 |
| Procedure 7. Replace a Failed 9372TX-E Switch | 74 |
| Procedure 8. Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch..... | 79 |
| Procedure 9. Replace a Failed Telco T5C-24GT | 82 |
| Procedure 10. Configure Cisco 3020 Switch (netConfig) | 88 |
| Procedure 11. Replace a Failed 3020 Switch | 93 |
| Procedure 12. Configure HP 6120XG Switch..... | 95 |
| Procedure 13. Configure HP 6125G Switch | 99 |
| Procedure 14. Configure HP 6125XLG Switch..... | 104 |
| Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch | 109 |
| Procedure 16. Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch | 113 |
| Procedure 17. Configure SNMP Communities and Trap Servers | 114 |
| Procedure 18. Configure SNMPv3 Security Model and Trap Servers | 118 |
| Procedure 19. Configure Access List to allow specific IP to access SNMPv2 | 124 |
| Procedure 20. Configure QoS (DSCP and/or CoS) on HP 6120XG Switches..... | 128 |
| Procedure 21. Configure Port Mirroring..... | 130 |
| Procedure 22. SwitchConfig to netConfig Repository Configuration | 134 |
| Procedure 23. Cisco Switch SwitchConfig to netConfig Migration | 144 |
| Procedure 24. HP 6120XG SwitchConfig to netConfig Migration | 146 |
| Procedure 25. Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig)..... | 149 |
| Procedure 26. Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig) | 151 |
| Procedure 27. Configure Brocade Switches..... | 153 |
| Procedure 28. Configure Zones in Brocade Switches..... | 157 |
| Procedure 29. Configure Brocade Switch XNMP Trap Target | 160 |
| Procedure 30. Set IP on Fibre Channel Disk Controllers | 164 |
| Procedure 31. Configure Fibre Channel Disk Controllers | 164 |

| | | |
|---------------|--|-----|
| Procedure 32. | Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers | 166 |
| Procedure 33. | Configure Advanced Settings on P2000 Fibre Channel Disk Controllers..... | 168 |
| Procedure 34. | Replace a Failed Disk in MSA 2012fc Array..... | 170 |
| Procedure 35. | Replace a Failed Disk in MSA P2000 Disk Array | 171 |
| Procedure 36. | BIOS Settings for HP Systems | 175 |
| Procedure 37. | BIOS Settings for Oracle Sun Systems | 178 |
| Procedure 38. | Configure Blade Server iLO Password for Administrator Account | 181 |
| Procedure 39. | Access the Server Virtual Serial Port..... | 182 |
| Procedure 40. | Configure Syscheck Default Route Ping Test..... | 183 |
| Procedure 41. | Prepare a System for Extended Power Outage..... | 183 |
| Procedure 42. | Bring Up a System After Extended Power Outage | 184 |
| Procedure 43. | Configure Initial OA IP | 185 |
| Procedure 44. | Configure Initial OA Settings Using the Configuration Wizard..... | 187 |
| Procedure 45. | Configure OA Security | 194 |
| Procedure 46. | Store OA Configuration on Management Server | 196 |
| Procedure 47. | Restore OA Configuration from Management Server..... | 199 |
| Procedure 48. | Replace Onboard Administrator..... | 201 |
| Procedure 49. | Update IPv4 Address | 203 |
| Procedure 50. | Update IPv6 Address | 206 |
| Procedure 51. | Add SNMP Trap Destination on OA..... | 209 |
| Procedure 52. | Disable SNMP Trap Destination on OA..... | 211 |
| Procedure 53. | Delete SNMP Trap Destination on OA..... | 211 |
| Procedure 54. | IPM the Management Server | 213 |
| Procedure 55. | Configure the TVOE Network | 218 |
| Procedure 56. | Deploy PMAC Guest..... | 227 |
| Procedure 57. | Set Up PMAC..... | 231 |
| Procedure 58. | Configure PMAC Application | 236 |
| Procedure 59. | Add Cabinet and Enclosure to the PMAC System Inventory..... | 240 |
| Procedure 60. | Edit an Enclosure in the PMAC System Inventory..... | 243 |
| Procedure 61. | Add ISO Images to the PMAC Image Repository | 245 |
| Procedure 62. | IPM Servers Using PMAC Application | 249 |
| Procedure 63. | Install/Upgrade Applications Using PMAC..... | 252 |
| Procedure 64. | Patch Applications Using PMAC..... | 254 |
| Procedure 65. | Install PMAC on Redundant DL360 or DL380 | 257 |
| Procedure 66. | Configure Management Server SNMP Trap Target | 260 |
| Procedure 67. | Install and Configure PMAC NetBackup Client..... | 261 |
| Procedure 68. | Add Rack Mount Server to the PMAC System Inventory | 263 |
| Procedure 69. | Edit Rack Mount Server in the PMAC System Inventory..... | 266 |
| Procedure 70. | Find and Add a Rack Mount Server to the PMAC System Inventory | 268 |
| Procedure 71. | Accept Upgrades Using PMAC | 272 |
| Procedure 72. | Reject Upgrades Using PMAC..... | 274 |
| Procedure 73. | Accept Patches Using PMAC | 276 |
| Procedure 74. | Reject Patches Using PMAC | 277 |
| Procedure 75. | Initialize PMAC Application Using CLI | 280 |

| | | |
|----------------|---|-----|
| Procedure 76. | Initialize PMAC Application Using the GUI | 282 |
| Procedure 77. | Configure PMAC Application Guest NetBackup Virtual Disk..... | 286 |
| Procedure 78. | Update the TVOE Host SNMP Community String from the GUI | 288 |
| Procedure 79. | Configure PMAC Application Guest Isoimages Virtual Disk..... | 293 |
| Procedure 80. | Generate a New Certificate Signing Request | 295 |
| Procedure 81. | Update an HTTPS Certificate | 297 |
| Procedure 82. | Import an HTTPS Certificate..... | 300 |
| Procedure 83. | Delete an HTTPS Certificate..... | 303 |
| Procedure 84. | Use the PMAC File Management System to Delete Files | 304 |
| Procedure 85. | Use the PMAC File Management System | 306 |
| Procedure 86. | Use the PMAC File Management System | 307 |
| Procedure 87. | Delete ISO Images from the PMAC Image Repository..... | 309 |
| Procedure 88. | Configure PMAC Domain Name System..... | 310 |
| Procedure 89. | Configure the PMAC into an Existing Single Sign-On (SSO) Domain..... | 315 |
| Procedure 90. | Configure an LDAP Server on the PMAC | 319 |
| Procedure 91. | Transfer Image from PMAC Repository to Other Servers | 321 |
| Procedure 92. | Configure SAN Storage Using PMAC Application | 324 |
| Procedure 93. | Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation | 326 |
| Procedure 94. | Create Guest Server Using PMAC Application..... | 327 |
| Procedure 95. | Delete Guest Server Using PMAC Application | 333 |
| Procedure 96. | Create Guest Server from Guest Archive Using PMAC Application..... | 335 |
| Procedure 97. | Back Up TVOE..... | 341 |
| Procedure 98. | Configure NTP on TPD-Based Application | 342 |
| Procedure 99. | Add SNMP Trap Destination on TPD-Based Application | 344 |
| Procedure 100. | Delete SNMP Trap Destination on TPD-Based Application | 345 |
| Procedure 101. | Install the NetBackup Client Application | 347 |
| Procedure 102. | Change SNMP Configuration Settings for iLO2..... | 349 |
| Procedure 103. | Change SNMP Configuration Settings for iLO3 and iLO4 | 350 |
| Procedure 104. | Change SNMP Configuration Settings for iLOM..... | 352 |
| Procedure 105. | Install NetBackup Client with nbAutoInstall | 353 |
| Procedure 106. | Install/Upgrade NetBackup Client with platcfg..... | 354 |
| Procedure 107. | Create LV and Filesystem for NetBackup Client Software | 358 |
| Procedure 108. | Migrate NetBackup Client to New Filesystem..... | 359 |
| Procedure 109. | Create NetBackup Client Config File | 360 |
| Procedure 110. | Enable Virtual Guest Watchdogs as Appropriate for the Application | 360 |
| Procedure 111. | Configure TVOE NetBackup Client..... | 361 |
| Procedure 112. | Copy a File from the Management Server to the PC Desktop | 362 |
| Procedure 113. | Install P2000 MSA USB Driver | 364 |
| Procedure 114. | Determine which Onboard Administrator is Active | 366 |
| Procedure 115. | Access a Remote Server Console | 368 |
| Procedure 116. | Attach an ISO Image to an HP Server Using iLO | 370 |
| Procedure 117. | Attach an ISO Image to an Oracle Rack Mount Server Using iLOM | 375 |
| Procedure 118. | Upgrade Cisco 4948 PROM | 378 |
| Procedure 119. | Disable SNMP on the OA | 385 |

| | |
|--|-----|
| Procedure 120. Downgrade Firmware on a 6125G Switch | 386 |
| Procedure 121. Downgrade Firmware on a 6125XLG Switch..... | 396 |
| Procedure 122. Change Switch Passwords (netConfig) | 407 |
| Procedure 123. Uninstall Symantec NetBackup Client | 408 |
| Procedure 124. Update the PMAC GSOAP Cipher List..... | 416 |
| Procedure 125. Update the TPD Provd Cipher List..... | 420 |
| Procedure 126. Increase the PMAC NetBackup Files System Size | 423 |
| Procedure 127. Turn Off Cipher List Before Backup Configuration/Restore Configuration/Upgrade Firmware Command..... | 430 |
| Procedure 128. Resume Cipher List After Backup Configuration/Restore Configuration/Upgrade Firmware Command..... | 430 |
| Procedure 129. Updating the SNMP Service on Existing Remote Servers on the PMAC Control Network | 434 |
| Procedure 130. Update the SNMP Service on the PMAC Server to Support SNMPv3..... | 435 |
| Procedure 131. Update the PMAC Messaging System to Support SNMPv3 | 436 |
| Procedure 132. Setting the PMAC security Levels..... | 437 |

1. Introduction

This document describes the procedures to configure third-party hardware and platform components that make up Platform 7.6.x configurable hardware components include HP ProLiant and Oracle rack mount servers (RMS), HP c7000 enclosures with HP blade servers, HP and Cisco switches, and HP external storage systems. Platform components include the firmware for various hardware components and the Platform Management and Configuration (PMAC) application to provision and manage those components when hosting feature applications.

Before executing any procedure in this document, power must be available to each component and all network cabling must be in place.

The procedures in this document are not presented in any specific order. Each procedure describes a discrete action. Application engineers need to reference individual procedures in their specific installation and configuration procedures. The application documentation provides the proper sequencing of procedures, application-specific supplemental steps, and passwords to use during the configuration.

1.1 References

For HP Blade and RMS firmware upgrades, Software Centric customers need the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes on <https://docs.oracle.com/en/industries/communications> under Platform documentation. Beyond the minimum version specified for the Platform below, the application dictates which Firmware Upgrade Packs to use.

[1] TPD Initial Product Manufacture Software Installation Procedure

[2] HP Solutions Firmware Upgrade Pack

The latest version is recommended if an upgrade is to be performed; otherwise, version 2.2.12 is the minimum. This pack includes both documentation and firmware media. For HP G6 server models, HP FUP 2.2.10 is the last HP FUP that provides support and is the minimum for G6 servers.

[3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

The latest version is recommended if an upgrade is performed; otherwise, version 2.2.12 is the minimum. For HP G6 server models, HP FUP 2.2.10 is the last HP FUP that provides support and is the minimum for G6 servers.

[4] Oracle Firmware Upgrade Pack Release Notes

The latest version is recommended if an upgrade is performed; otherwise, version 3.1.8 is the minimum.

[5] Oracle Firmware Upgrade Pack Upgrade Guide, version 3.1.8.

[6] PMAC Incremental Upgrade Procedure, Release 6.6.

[7] PMAC Disaster Recovery, Release 6.6.

1.2 Acronyms

Table 1. Acronyms

| Acronym | Definition |
|---------|------------------------------|
| AES | Advanced Encryption Standard |
| BIOS | Basic Input Output System |
| CA | Certificate Authority |
| CSR | Certificate Signing Request |

| Acronym | Definition |
|------------|--|
| DES | Data Encryption Algorithm |
| DNS | Domain Name System |
| DSCP | Differentiated Services Code Point, a form of QoS |
| DVD | Digital Versatile Disc |
| EBIPA | Enclosure Bay IP Addressing |
| FMA | File Management Area |
| FQDN | Fully Qualified Domain Name |
| FRU | Field Replaceable Unit |
| HP c-Class | HP blade server offering |
| HP FUP | HP Firmware Upgrade Pack |
| iLO | Integrated Lights Out remote management port |
| iLOM | Integrated Lights Out Manager |
| IE | Internet Explorer |
| IPM | Initial Product Manufacture – the process of installing TPD on a hardware platform |
| MD5 | Message Digest Algorithm 5 |
| MP | Message Processing Server |
| MSA | Modular Smart Array |
| NAPD | Network Architecture Planning Diagram |
| NMS | Network Management System |
| NO | Network OAM&P Server |
| OA | HP Onboard Administrator |
| OAM&P | Operations, Administration, Maintenance, and Provisioning |
| OS | Operating System (e.g. TPD) |
| OSDC | Oracle Software Delivery Cloud |
| PMAC | Platform Management and Configuration |
| QOS | Quality of Service |
| RMS | Rack Mount Server |
| SAN | Storage Area Network |
| SFTP | Secure File Transfer Protocol |
| SHA | Secure Hash Algorithm |
| SNMP | Simple Network Management Protocol |
| SO | System OAM&P server |
| SSO | Single Sign On |
| TPD | Tekelec Platform Distribution |
| TVOE | Tekelec Virtual Operating Environment |

| Acronym | Definition |
|---------|---------------------|
| VSP | Virtual Serial Port |

1.3 Terminology

| Term | Definition |
|------------------------|--|
| Community String | An SNMP community string is a text string used to authenticate messages sent between a management station and a device (the SNMP agent). The community string is included in every packet that is transmitted between the SNMP manager and the SNMP agent. |
| Domain Name System | A system for converting hostnames and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol |
| Management Server | An HP ProLiant DL 360/DL 380 or Oracle RMS that has physical connectivity required to configure switches and may host the PMAC application or serve other configuration purposes. |
| NetBackup Feature | Feature that provides support of the Symantec NetBackup client utility on an application server. |
| Non-Segregated Network | Network interconnect where the control and management, or customer, networks use the same physical network. |
| PMAC | An application that supports platform-level capability to manage and provision platform components of the system, so they can host applications. |
| Segregated Network | Network interconnect where the control and management, or customer, networks use separate physical networks. |
| Server | A generic term to refer to a server, regardless of underlying hardware, be it physical hardware or a virtual TVOE guest server. |
| Software Centric | A term used to differentiate between customers buying both hardware and software from Oracle, and customers buying only software. |
| Virtual PMAC | Additional term for PMAC - used in networking procedures to distinguish activities done on a PMAC guest and not the TVOE host running on the Management server. |

1.4 How to Use this Document

Although this document is primarily to be used as an initial installation guide, its secondary purpose is as a reference for disaster recovery procedures. When executing this document for either purpose, there are a few points to help ensure the user understands the document's intent. These points are as follows:

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

If a procedural step fails to execute successfully, stop and contact Oracle's Help Center for assistance before attempting to continue. See Appendix T for information on contacting My Oracle Support (MOS).

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

- Any sub-steps within a step are referred to as step X.Y. The example in Figure 1 shows steps 1 through 3, and step 3.1.
- GUI menu items, action links, and buttons to be clicked on are in bold Arial font.

- GUI fields and values to take note of during a step are in bold Arial font.
- Where it is necessary to identify the server explicitly on which a particular step is to be taken, the server name is given in the title box for the step (for example, **ServerX** in step 2 Figure 1).

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

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

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

| | Title | Directive/Result Step |
|--------------------------|--|---|
| <input type="checkbox"/> | 1. Change directory | Change to the backout directory. <code>\$ cd /var/TKLC/backout</code> |
| <input type="checkbox"/> | 2. ServerX : Connect to the console of the server | Establish a connection to the server using cu on the terminal server/console. <code>\$ cu -l /dev/ttyS7</code> |
| <input type="checkbox"/> | 3. Verify Network Element data | View the Network Elements configuration data; verify the data; save and print report. Select Configuration > Network Elements to view Network Elements Configuration screen. |

Figure 1. Example of a Procedure Step Used in This Document

2. Acquiring Firmware

Several procedures in this document pertain to the upgrading of firmware on various servers and hardware devices that are part of the Platform configuration.

Platform servers and devices requiring possible firmware updates are:

- HP c7000 Blade System Enclosure Components:
 - Onboard Administrator
 - 1Gb Ethernet Pass-Thru Module
 - Cisco 3020 Enclosure Switches
 - HP6120XG Enclosure Switches
 - HP6125G Enclosure Switches
 - HP6125XLG Enclosure Switches
 - Brocade Fibre Channel Switches
 - Blade Servers (BL460/BL620)
- HP Rack Mount Servers (DL360 / DL380)
- Oracle Rack Mount Servers
- HP External Storage Systems
 - MSA 2012fc
 - D2200sb (Storage Blade)

- D2220sb (Storage Blade)
- D2700
- P2000
- Cisco 4948/4948E/4948E-F Rack Mount Network Switches
- Cisco 9372TX-E Rack Mount Network Switches

2.1 HP

Software Centric Customers do not receive firmware upgrades through Oracle. Instead, refer to the HP Solutions Firmware Upgrade Pack, Software Centric Release Notes on <http://docs.oracle.com> at **Industries > Communications > Platforms > Tekelec**.

For customers who purchased their hardware through Oracle, or previously Tekelec, the required firmware and documentation for upgrading the firmware on HP hardware systems and related components are distributed as the HP Solutions Firmware Upgrade Pack 2.2.12.

The minimum firmware release required for PMAC 6.6 is HP Solutions Firmware Upgrade Pack 2.2.12. For HP G6 server models, HP FUP 2.2.10 is the last HP FUP that provides support and is the minimum for G6 servers.

Each version of the HP Solutions Firmware Upgrade Pack contains multiple items including media and documentation, which are used to upgrade HP firmware. The two pieces of required documentation provided in the HP Solutions Firmware Upgrade Pack 2.x.x releases are:

- HP Solutions Firmware Upgrade Pack Upgrade Guide
- HP Solutions Firmware Upgrade Pack Release Notes

The two pieces of required firmware media provided in the HP Solutions Firmware Upgrade Pack 2.2.12 releases are:

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC Firmware ISO image
- Refer to the [4] Oracle Firmware Upgrade Pack Release Notes

2.2 Oracle Rack Mount Server

The Oracle Firmware Upgrade Pack (FUP) consists of documentation used to assist in the upgrading of Oracle rack mount servers. The pack consists of an *Upgrade Guide* and *Release Notes*. The current minimum supported firmware release for PMAC 6.6 is 3.1.8. However, if a firmware update is required, it is recommended to use the latest available release. Firmware components can be downloaded from My Oracle Support at <https://support.oracle.com>. Refer to the appropriate FUP Release Notes for directions on how to acquire the firmware.

3. Network Procedures

3.1 Configure netConfig Repository

This procedure configures the netConfig repository for all required services and for each switch to be configured.

Prerequisites:

- 8.1 IPM Management Server
- If the PMAC is included in the installation:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC

At any time, you can view the contents of the netConfig repository by using one of the following commands:

- For switches, use the command:

```
sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
```
- For services, use the command:

```
sudo /usr/TKLC/plat/bin/netConfig --repo listServices
```

Users returning to this procedure after initial installation should run the above commands and note any devices and/or services that have already been configured. Duplicate entries cannot be added; if changes to a device repository entry are required, use the `editDevice` command. If changes to a services repository entry are necessary, you must delete the original entry first and then add the service again.

IPv4 and IPv6

Platform now supports configuration using IPv4 or IPv6 addresses through netConfig. Wherever IP addresses are required for networking procedures in section 3.1, IPv4 or IPv6 may be used. Commands such as ping or ssh may also be used in these procedures, where for IPv6 cases may need to be `ping6` or `ssh -6` as needed.

Terminology

The term **netConfig server** refers to the entity where netConfig is executed. This may be a virtualized or physical environment. **Management server** may also accurately describe this location, but has been historically used to describe the physical environment, while **Virtual PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments allow for future simplification of network configuration procedures.

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Fill in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

| Variable | Value |
|--|---------------|
| <management_server_iLO_IP> | |
| <management_server_mgmt_IP_address> | |
| <netConfig_server_mgmt_IP_address> | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> See application documentation | |
| <serial console type> | U=USB, c=PCIe |

For the first aggregation switch (4948, 4948E, or 4948E-F), fill in the appropriate value for this site:

| Variable | Value |
|--|-------|
| <switch_hostname> From NAPD or output from <code>listDevices</code> | |

| Variable | Value |
|---|-------|
| command | |
| <device_model> | |
| <console_name> | |
| <switch_console_password> See referring application documentation | |
| <switch_platform_username> | |
| <switch_platform_password> See referring application documentation | |
| <switch_enable_password> See referring application documentation | |
| <switch_mgmt_IP_address> CIDR format | |
| <switch_mgmt_netmask> | |
| <mgmt_VLAN_ID> | |
| <control_VLAN_ID> | |
| <IOS_filename> | |
| <IP_version> | |

For the second aggregation switch (4948, 4948E, or 4948E-F), fill in the appropriate value for this site:

| Variable | Value |
|---|-------|
| <switch_hostname> | |
| <device_model> | |
| <console_name> | |
| <switch_console_password> See referring application documentation | |
| <switch_platform_username> | |
| <switch_platform_password> See referring application documentation | |
| <switch_enable_password> See referring application documentation | |
| <switch_mgmt_IP_address> | |
| <switch_mgmt_netmask> | |
| <mgmt_VLAN_ID> Value gathered from NAPD | |
| <control_VLAN_ID> | |
| <IOS_filename> | |
| <IP_version> | |

For each enclosure switch (6120XG, 6125G, 6125XLG, or 3020), fill in the appropriate value for this site (make as many copies of this table as needed).

| Variable | Value |
|--|--------------------|
| <switch_hostname> | |
| <enclosure_switch_IP> | |
| <switch_platform_username> | |
| <switch_platform_password> | |
| <switch_enable_password> See referring application documentation | |
| <io_bay> | |
| <OA1_enX_IP_address> | X= the enclosure # |
| <OA_password> | |
| <FW_image> FW file used in firmware upgrade/switch replacement/or initial install | |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Management Server iLO: Login | Log into the management server iLO on the remote using the password provided by the application following Appendix E.1 Access a Server Console Remotely. |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|--|--|---|
| <p>2. <input type="checkbox"/></p> | <p>Management Server: Pre-check</p> | <p>If the installation is not designed for a virtual PMAC, skip to the next step. If there is a virtual PMAC, log into the console.</p> <ol style="list-style-type: none"> 1. Verify virtual PMAC installation by issuing the following commands as admusr on the management server: <pre>\$ sudo /usr/bin/virsh list --all</pre> <pre>Id Name State 6 vm-pmac1A running</pre> 2. If this command provides no output, it is likely that a virtual instance of PMAC is not installed. <ul style="list-style-type: none"> • If there is a virtual PMAC, log into the console of the virtual PMAC. • If the installation is not designed for a virtual PMAC, skip to the next step. 3. From the management server, log into the console of the virtual PMAC instance found above. <p>Example:</p> <pre>\$ sudo /usr/bin/virsh console vm-pmac1A</pre> <pre>Connected to domain vm-pmac1A</pre> <pre>Escape character is ^]</pre> <pre><Press ENTER key></pre> <pre>CentOS release 6.2 (Final)</pre> <pre>Kernel 2.6.32-220.7.1.el6prere16.0.0_80.13.0.x86_64 on an x86_64</pre> <p>If the root user is already logged in, log out and log back in as admusr.</p> <pre>[root@pmac ~]# logout</pre> <pre>vm-pmac1A login: admusr</pre> <pre>Password:</pre> <pre>Last login: Fri May 25 16:39:04 on ttyS4</pre> <ul style="list-style-type: none"> • If this command fails, it is likely that a virtual instance of PMAC is not installed. • If this is unexpected, refer to application documentation or My Oracle Support (MOS). |
| <p>3. <input type="checkbox"/></p> | <p>netConfig Server: Check switch templates directory</p> | <p>Make sure the switch templates directory exists.</p> <pre>\$ /bin/ls -i /usr/TKLC/smac/etc/switch/xml</pre> <p>If the command returns an error:</p> <pre>ls: cannot access /usr/TKLC/smac/etc/switch/xml/: No such file or directory</pre> <p>Create the directory:</p> <pre>\$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/xml</pre> <p>Change directory permissions:</p> <pre>\$ sudo /bin/chmod go+rx /usr/TKLC/smac/etc/switch/xml</pre> <p>Change directory ownership:</p> <pre>\$ sudo /bin/chown -R pmacd:pmacbackup /usr/TKLC/smac/etc/switch</pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|--|--|--|
| <p>4. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig repository with ssh information</p> | <p>1. Use netConfig to create a repository entry that uses the ssh service. This command provides the user with several prompts. Modify the prompts with <variables> as the answers, which are site specific. The other prompts, which do not have a <variable> shown as the answer, must be entered EXACTLY as they are shown here.</p> <pre data-bbox="565 472 1412 835"> \$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service Service type? (tftp, ssh, conserver, oa) ssh Service host? <netConfig_server_mgmt_IP_address> Enter an option name <q to cancel>: user Enter the value for user: <switch_backup_user> Enter an option name <q to cancel>: password Enter the value for password: <switch_backup_user_password> Verify Password: <switch_backup_user_password> Enter an option name <q to cancel>: q Add service for ssh_service successful [admusr@minilab-pmac-1~]\$ sudo netConfig --repo addService name=ssh_service Service type? (dhcp, oa, oobm, ssh, tftp, conserver) ssh Service host? 1.2.3.4 Enter the value for user: admusr Enter the value for password: <admusr_password> Verify Password: <admusr_password> Add service for ssh_service successful </pre> <p>2. To ensure you entered the information correctly, use the following command and inspect the output, which is similar to the one shown below.</p> <pre data-bbox="565 1264 1339 1522"> \$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service Service Name: ssh_service Type: ssh Host: 10.250.8.4 Options: password: C20F7D639AE7E7 user: admusr </pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|--|---|--|
| <p>5. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig repository with TFTP information</p> | <p>Note: If there are no new Cisco (3020, 4948, 4948E or 4948E-F) switches to be configured, go to the next step.</p> <p>Use netConfig to create a repository entry that uses the tftp service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> For a PMAC system: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service Service type? [dhcp, oa, oobm, ssh, tftp, conserver] tftp Service host? <netConfig_server_mgmt_IP_address> Directory on host? /var/TKLC/smac/image/ Add service for tftp_service successful</pre> For a non-PMAC system: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service Service type? [tftp, ssh, conserver, oa] tftp Service host? <netConfig_server_mgmt_IP_address> Directory on host? /var/lib/tftpboot/ Add service for tftp_service successful</pre> |
| <p>6. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig repository with OA information</p> | <p>Note: If there are no new HP 6125G/6125XLG/6120XG switches to configure, go to the next step.</p> <p>Use netConfig to create a repository entry that uses the OA service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=oa_service_en<enclosure #> Service type? [dhcp, oa, oobm, ssh, tftp, conserver]? oa Primary OA IP? <OA1_enX_ip_address> Secondary OA IP? <OA2_enX_ip_address> OA username? root OA password? password Verify password:<OA_password> Add service for oa_service successful</pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|-----------------|--|---|
| <p>7. □</p> | <p>netConfig Server: Run conserverSetup command</p> | <pre>\$ sudo /usr/TKLC/plat/bin/conserverSetup -<serial console type> -s <management_server_mgmt_IP_address></pre> <p>You are asked for the platcfg credentials. Example:</p> <pre>[admusr@vm-pmac1A]\$ sudo /usr/TKLC/plat/bin/conserverSetup -u - s <management_server_mgmt_IP_address></pre> <p>Enter your platcfg username, followed by [ENTER]:platcfg Enter your platcfg password, followed by [ENTER]:<platcfg_password></p> <p>Checking Platform Revision for local TPD installation... The local machine is running: Product Name: PMAC Base Distro Release: 7.0.0.0.0_86.1.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: TVOE Base Distro Release: 7.0.0.0.0_86.2.0 Configuring switch 'switch1A_console' console server...Configured. Configuring switch 'switchBA_console' console server...Configured. Configuring iptables for port(s) 782...Configured. Configuring iptables for port(s) 1024:65535...Configured. Configuring console repository service... Repo entry for "console_service" already exists; deleting entry for: Service Name: console_service Type: conserver Host: <management_server_mgmt_IP_address> ...Configured. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth02 <ul style="list-style-type: none"> • If this command fails, contact My Oracle Support (MOS). • Verify the output of the script. • Verify your Product Release is based on Tekelec Platform 7.4. • Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps. </p> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|--|--|---|
| <p>8. <input type="checkbox"/></p> | <p>netConfig Server: Mount the HP Misc Firmware ISO</p> | <p>Note: If this is a Software Centric deployment, skip this step and proceed to step 9.</p> <pre>\$ sudo /bin/mount -o loop /var/TKLC/upgrade/<misc_ISO> /mnt/upgrade</pre> <p>Example:</p> <pre>\$ sudo /bin/mount -o loop /var/TKLC/upgrade/872-2161-113-2.1.10_10.26.0.iso/mnt/upgrade</pre> |
| <p>9. <input type="checkbox"/></p> | <p>netConfig Server: Copy Cisco switch</p> | <p>Note: If there are no Cisco switches, skip to the next step.</p> <p>Copy Cisco switch FW to the <code>tftp_directory</code>.</p> <p>Note: If this is a Software Centric deployment, the customer must place the FW files for the Cisco switches (C3020, 4948/E/E-F) into the tftp directory listed below. Otherwise, perform the commands to copy the file from the FW ISO.</p> <p>For each Cisco switch model (C3020, 4948/E/E-F) present in the solution, copy the FW identified by <code><FW_image></code> in the aggregation switch variable table (4948) or enclosure switch variable table (C3020) to the <code>tftp_service</code> directory and change the permissions of the file:</p> <ul style="list-style-type: none"> For a PMAC system: <pre><tftp_directory> = /var/TKLC/smac/image/</pre> For a non-PMAC system: <pre><tftp_directory> = /var/lib/tftpboot/ \$ sudo /bin/cp /mnt/upgrade/files/<FW_image> <tftp_directory> \$ sudo /bin/chmod 644 <tftp_directory>/<FW_image></pre> <p>Example:</p> <pre>\$ sudo /bin/cp /mnt/upgrade/files/cat4500e-entservicesk9-mz.122-54.XO.bin /var/TKLC/smac/image/ \$ sudo /bin/chmod 644 /var/TKLC/smac/image/cat4500e-entservicesk9-mz.122-54.XO.bin</pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|---|---|---|
| <p>10. <input type="checkbox"/></p> | <p>netConfig Server: Copy HP switch</p> | <p>Note: If there are no HP switches, skip to the next step.</p> <p>Copy HP switch FW to the <code>ssh</code> directory</p> <p>Note: If this is a Software Centric deployment, the customer must place the FW files for the HP switches into the <code>ssh</code> directory listed below. Otherwise, perform the commands to copy the file from the FW ISO.</p> <p>For each HP switch model (HP6125G/XLG, HP6120XG) present in the solution, copy the FW identified by <code><FW_image></code> in the enclosure switch variable tables to the <code>ssh_service</code> directory and change the permissions of the file:</p> <pre>\$ sudo /bin/cp /mnt/upgrade/files/<FW_image> ~<switch_backup_user>/ \$ sudo /bin/chmod 644 ~<switch_backup_user>/<FW_image></pre> <p>Example:</p> <pre>\$ sudo /bin/cp /mnt/upgrade/files/Z_14_37.swi ~admusr/ \$ sudo /bin/chmod 644 ~admusr/Z_14_37.swi</pre> |
| <p>11. <input type="checkbox"/></p> | <p>netConfig Server: Unmount ISO</p> | <pre>\$ sudo /bin/umount /mnt/upgrade</pre> |
| <p>12. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig repository with aggregation switch information</p> | <p>Note: If there are no new aggregation switches to configure, go to the next step.</p> <p>Use netConfig to create a repository entry for each switch. This command provides the user with several prompts. The prompts shown with <code><variables></code> as the answers are site specific that the user MUST modify. Other prompts that do not have a <code><variable></code> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> The <code><device_model></code> can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact My Oracle Support (MOS). The device name must be 20 characters or less. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? Cisco Device Model? <device_model> What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address> Is the management interface a port or a vlan? [vlan]: [Enter] What is the VLAN ID of the management VLAN? [2]: [mgmt_vlanID] What is the name of the management VLAN? [management]: [Enter] What switchport connects to the management server? [GE40]: [Enter] What is the switchport mode (access trunk) for the management server port? [trunk]: [Enter] What are the allowed vlans for the management server port?</pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|------|-----------|--|
| | | <pre> [1,2]: <control_vlanID>, <mgmt_vlanID> Enter the name of the firmware file [cat4500e-entservicesk9- mz.122-54.XO.bin]: <IOS_filename> Firmware file to be used in upgrade: <IOS_filename> Enter the name of the upgrade file transfer service: tftp_service File transfer service to be used in upgrade: tftp_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? console_service What is the name of the console for OOB access? <console name> What is the platform access username? <switch_platform_username> What is the device console password? <switch_console_password> Verify password: <switch_console_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_enable_password> Verify password: <switch_enable_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_IP_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: console_service Device named <switch_hostname> successfully added. To check you entered the information correctly, use the following command: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> and check the output, which is similar to the one shown: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> Device: <switch_hostname> Vendor: Cisco Model: <device_model> FW Ver: 0 FW Filename: <IOS_image> FW Service: tftp_service </pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|---|--|--|
| | | <pre> Initialization Management Options mgmtIP: <switch_mgmt_IP_address> mgmtInt: vlan mgmtVlan: <mgmt_vlanID> mgmtVlanName: management interface: GE40 mode: trunk allowedVlans: <control_vlanID>, <mgmt_vlanID> Access: Network: <switch_mgmt_IP_address> Access: OOB: Service: console_service Console: <console_name> Init Protocol Configured Live Protocol Configured Repeat this step for each 4948/4948E/4948 E-F, using appropriate values for those switches. </pre> |
| <p>13. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig repository with 3020 switch information</p> | <p>Notes:</p> <ul style="list-style-type: none"> • If there are no new 3020s to be configured, go to the next step. • The Cisco 3020 is not compatible with IPv6 management configuration. <p>Use netConfig to create a repository entry for each 3020. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? Cisco Device Model? 3020 What is the management address? <enclosure_switch_ip> Enter the name of the firmware file [cbs30x0-ipbasek9-tar.122-58.SE1.tar]: <FW_image> Firmware file to be used in upgrade: <IOS_image> Enter the name of the upgrade file transfer service: <tftp_service> File transfer service to be used in the upgrade: <tftp_service> Should the init network adapter be added (y/n)? y Adding netBootInit protocol for <switch_hostname> using network... </pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|---|--|--|
| | | <pre> Network device access already set: <enclosure_switch_ip> What is the platform access username? <switch_platform_username> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_enable_password> Verify password: <switch_enable_password> Should the init file adapter be added (y/n)? y Adding netBootInit protocol for <switch_hostname> using file... What is the name of the service used for TFTP access? tftp_service Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <enclosure_switch_ip> Device named <switch_hostname> successfully added. To check you entered the information correctly, use the following command: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> and check the output, which is similar to the one shown below. \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> Device: <switch_hostname> Vendor: Cisco Model: <device_model> FW Ver: 0 FW Filename: <FW_image> FW Service: tftp_service Access: Network: <enclosure_switch_IP> Init Protocol Configured Live Protocol Configured Repeat this step for each 3020, using appropriate values for those 3020s. Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. or the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image: WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location. </pre> |
| <p>14. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig</p> | <p>Note: If there are no 6120XGs to be configured, stop and continue with the appropriate switch configuration procedure.</p> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|------|--|--|
| | repository with HP 6120XG switch information | <p>Use netConfig to create a repository entry for each 6120XG. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? HP Device Model? 6120 What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address> Enter the name of the firmware file [Z_14_37.swi]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service: ssh_service File transfer service to be used in upgrade: ssh_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? oa_service_en<enclosure #> What is the name of the console for OOB access? <io_bay> What is the platform access username? <switch_platform_username> What is the device console password? <switch_platform_password> Verify password: <switch_platform_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_platform_password> Verify password: <switch_platform_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_IP_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: oa_service_en<enclosure #> Device named <switch_hostname> successfully added The image is being unpacked and validated. This takes approximately 4 </pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|---|--|--|
| | | <p>minutes. Once the unpacking, validation, and rebooting have completed, you are returned to the normal prompt. Proceed with the next step.</p> <p>To verify you entered the information correctly, use the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname></pre> <p>and check the output, which is similar to the one shown:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname></pre> <pre>Device: <switch_hostname> Vendor: HP Model: 6120 FW Ver: 0 FW Filename: <FW_image> FW Service: ssh_service Initialization Management Options mgmtIP: <enclosure_switch_IP> Access: Network: <enclosure_switch_IP> Access: OOB: Service: oa_service Console: <console_name> Init Protocol Configured Live Protocol Configured</pre> <p>Repeat this step for each 6120, using appropriate values for those 6120s.</p> <p>Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image:</p> <p style="text-align: center;">WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.</p> |
| <p>15. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig repository with HP 6125G switch information</p> | <p>Note: If there are no 6125Gs to be configured, stop and continue with the appropriate switch configuration procedure.</p> <p>Use netConfig to create a repository entry for each 6125G. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? HP</pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|------|-----------|--|
| | | <pre> Device Model? 6125 What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management? <switch_mgmt_IP_address> Enter the name of the firmware file [6125-CMW520-R2105.bin]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service: ssh_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? oa_service_en<enclosure #> What is the name of the console for OOB access? <io_bay> What is the platform access username? <switch_platform_username> What is the device console password? <switch_platform_password> Verify password: <switch_platform_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_platform_password> Verify password: <switch_platform_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_IP_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: oa_service_en<enclosure #> Device named <switch_hostname> successfully added. Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image: WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location. To verify you entered the information correctly, use the following command: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> and check the output, which is similar to the one shown: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice </pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|-------------------------------------|--|--|
| | | <pre> name=<switch_hostname> Device: <switch_hostname> Vendor: HP Model: 6125 FW Ver: 0 FW Filename: <FW_image> FW Service: ssh_service Access: Network: <enclosure_switch_IP> Access: OOB: Service: oa_service Console: <io_bay> Init Protocol Configured Live Protocol Configured </pre> |
| <p>16. <input type="checkbox"/></p> | <p>netConfig Server: Set up netConfig repository with HP 6125XLG switch information</p> | <p>Note: If there are no 6125XLGs to be configured, stop and continue with the appropriate switch configuration procedure.</p> <p>Use netConfig to create a repository entry for each 6125XLG. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> • If you do not know any of the required answers, stop now and contact My Oracle Support (MOS). • The device name must be 20 characters or less. <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? HP Device Model? 6125XLG What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address> Enter the name of the firmware file [6125XLG-CMW710-R2403.ipe]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service: ssh_service File transfer service to be used in upgrade: ssh_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? oa_service_en<enclosure#> What is the name of the console for OOB access? <io_bay> What is the platform access username? <switch_platform_username> </pre> |

Procedure 1. Configure netConfig Repository

| Step | Procedure | Result |
|------|-----------|--|
| | | <pre> What is the device console password? <switch_platform_password> Verify password: <switch_platform_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_platform_password> Verify password: <switch_platform_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_IP_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: oa_service_en<enclosure #> Device named <switch_hostname> successfully added Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. For the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image: WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location. To verify you entered the information correctly, use the following command: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> and check the output, which is similar to the one shown: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> Device: <switch_hostname> Vendor: HP Model: 6125XLG FW Ver: 0 FW Filename: <FW_image> FW Service: ssh_service Access: Network: <enclosure_switch_IP> Access: OOB: Service: oa_service Console: <io_bay> Init Protocol Configured </pre> |

3.2 Aggregation Switch — netConfig Procedures

3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)

This procedure configures 4948/4948E/4948E-F switches with an appropriate IOS and configuration from a single management server and virtual PMAC for use with the c-Class or RMS platform.

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC
- Application management network interfaces must be configured on the management servers before executing this procedure.
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate value from [2] HP Solutions Firmware Upgrade Pack.

| Variable | Cisco 4948 | Cisco 4948E | Cisco 4948E-F |
|------------------|------------|-------------|---------------|
| <IOS_image_file> | | | |

Fill in the appropriate value for this site.

| Variable | Value |
|---|--------|
| <switch_platform_username> See referring application documentation | |
| <switch_platform_password> | |
| <switch_console_password> See referring application documentation | |
| <switch_enable_password> See referring application documentation | |
| <management_server_mgmt_IP_address> | |
| <pmac_mgmt_IP_address> | |
| <switch_mgmtVLAN_ID> | |
| <switch1A_mgmtVLAN_IP_address> | |
| <mgmt_Vlan_subnet_ID> | |
| <netmask> | |
| <switch1B_mgmtVLAN_IP_address> | |
| <switch_Internal_VLAN_list> | |
| <management_server_mgmtInterface> | |
| <management_server_iLO_IP> | |
| <customer_supplied_ntp_server_address> | |
| <platcfg_password> Initial password as provided by Oracle | |
| <management_server_mgmtInterface> Value gathered from NAPD | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> Check application documentation | |

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Uplinks must be disconnected from the customer network before executing this procedure. One of the steps in this procedure instructs when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.
- Filenames and sample command line input/output throughout this procedure do not specifically reference the 4948E-F. Template settings are identical between the 4948E and 4948E-F. The original 4948 switch – as opposed to the 4948E or the 4948E-F is referred to simply by the model number 4948. Where all three switches are referred to, this is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact My Oracle Support (MOS) for assistance.

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Virtual PMAC: Verify IOS image is on the system | Determine if the IOS image for the 4948/4948E/4948E-F is on the PMAC. <pre>\$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file></pre> If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes. |
| 2. <input type="checkbox"/> | Virtual PMAC: Modify P&C feature to allow TFTP | Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm editFeature -- featureName=DEVICE.NETWORK.NETBOOT --enable=1</pre> <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures</pre> Note: Ignore the sentry restart instructions. Note: This may take up to 60 seconds to complete. |

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|-----------------|---|---|
| <p>3. □</p> | <p>Virtual PMAC > Management Server: Manipulate host server physical interfaces</p> | <p>Exit from the virtual PMAC console, by pressing Ctrl-] and you are returned to the server prompt.</p> <p>Ensure the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>.</p> <pre>\$ sudo /usr/bin/virsh console vm-pmac1A</pre> <p>Note: On a TVOE host, if you open the virsh console, i.e., <code>\$ sudo virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or output is not correct, then more than likely there is a stuck virsh console command already being run on the TVOE host. Exit the virsh console, and run <code>ps -ef grep virsh</code>, then kill the existing process <code>\$ sudo kill -9 <PID></code>. Execute the <code>\$ sudo virsh console X</code> command again. Your console session should now run as expected.</p> |
| <p>4. □</p> | <p>Management Server: Determine if switch1A PROM upgrade is required</p> | <p>Note: ROM and PROM are intended to have the same meaning for this procedure.</p> <p>Connect to switch1A and check the PROM version.</p> <p>Connect serially to switch1A by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter `^Ec?' for help] Press Enter Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> <p>Note: If the console command fails, contact Error! Bookmark not defined..</p> <p>Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing <Ctrl-e><c><.> and you are returned to the server prompt.</p> <p>Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.</p> |

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|--|---|--|
| <p>5. <input type="checkbox"/></p> | <p>Virtual PMAC: Extract configuration files</p> | <p>Extract the configuration files from the ZIP file copied in 9. of Procedure 1.</p> <pre>\$ cd /usr/TKLC/smac/etc \$ sudo unzip DSR_NetConfig_Templates.zip \$ sudo chown -R admusr.admgrp DSR_NetConfig_Templates</pre> <p>This creates a directory called DSR_NetConfig_Templates, which contains the configuration files for all the supported deployments. Copy the necessary init file from init/Aggregation and the necessary config files from config/TopoX (where X refers to the appropriate topology) using the following commands. Make sure to replace X with the appropriate Topology number.</p> <p>Note: The following workaround is needed:</p> <p>Remove the double right brackets for:</p> <p>DSR_NetConfig_Templates/Topo1_L2/4948E-F_L2_configure.xml: <option name="type">access</option>></p> <p>DSR_NetConfig_Templates/Topo4/6125XLG_Pair-2_template_configure.xml: <!-- Multiple VLANs can be entered by stringing the VLANs in the setAllowedVlans option, i.e., 1-5 or 1,2,3,4,5 -->></p> <p>DSR_NetConfig_Templates/Topo1_L3/3020_template_configure.xml: <!-- 'mode' is required on Cisco when adding interfaces -->></p> <p>Replace <configure> with <configure apiVersion="1.1"> within: DSR_NetConfig_Templates/utility/addQOS_trafficeTemplate_6120XG.xml</p> <pre># sudo cp DSR_NetConfig_Templates/init/Aggregation/* /usr/TKLC/smac/etc/switch/xml/ # sudo cp DSR_NetConfig_Templates/config/TopoX/* /usr/TKLC/smac/etc/switch/xml/</pre> |
| <p>6. <input type="checkbox"/></p> | <p>Management Server: Modify switch1A_4948_4948E.xml and switch1B_4948_4948E.xml</p> | <p>Modify switch1A_4948_4948E_init.xml and switch1B_4948_4948E_init.xml files for information needed to initialize the switch.</p> <p>Update the init.xml files for all values preceded by a dollar sign. For example, if a value has <code>\$some_variable_name</code>, that value is modified and the dollar sign must be removed during the modification.</p> <p>When done editing the file, save and exit to return to the command prompt.</p> |
| <p>7. <input type="checkbox"/></p> | <p>Management Server: Modify 4948E-F_configure.xml</p> | <p>Modify 4948E-F_configure.xml for information needed to configure the switches.</p> <p>Update the configure.xml file for all values preceded by a dollar sign. For example, if a value has <code>\$some_variable_name</code>, that value is modified and the dollar sign must be removed during the modification.</p> <p>When done editing the file, save and exit to return to the command prompt.</p> <p>Note: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the Cisco 4948E-F aggregation switches. This function must be configured for IPv4.</p> |

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---|---|--|
| <p>8. <input type="checkbox"/></p> | <p>Management Server: Initialize switch1A</p> | <p>Initialize switch1A by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml 1</pre> <p>Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</p> <p>Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns you to the prompt. Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname Hostname: switch1A</pre> |
| <p>9. <input type="checkbox"/></p> | <p>Management Server: Verify IOS image</p> | <p>Verify the switch is using the proper IOS image per Platform version by issuing the following commands:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> |
| <p>10. <input type="checkbox"/></p> | <p>Virtual PMAC > Management Server: Manipulate host server physical interfaces</p> | <p>Exit from the virtual PMAC console, by pressing Ctrl-] and you are returned to the server prompt.</p> <p>Ensure the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>.</p> <p>Connect to the Virtual PMAC by logging into the console of the virtual PMAC instance found in 2. of Procedure 1.</p> <pre>\$ sudo /usr/bin/virsh console vm-pmac1A</pre> <p>Note: On a TVOE host, if you open the virsh console, for example, <code>\$ sudo /usr/bin/virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or the output is not correct, then there is likely a stuck virsh console command already being run on the TVOE host. Exit out of the virsh console, run <code>ps -ef grep virsh</code>, and then kill the existing process, run <code>kill -9 <PID></code>. Then execute the <code>virsh console X</code> command. Your console session should now run as expected.</p> |

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---|---|---|
| <p>11. <input type="checkbox"/></p> | <p>Management Server: Determine if switch1B PROM upgrade is required</p> | <p>Note: ROM AND PROM are intended to have the same meaning for this procedure.</p> <p>Connect to switch1A and check the PROM version.</p> <p>Connect serially to switch1A by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter '^Ec?' for help] Press Enter Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> <p>Note: If the console command fails, contact Error! Bookmark not defined..</p> <p>Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing <Ctrl-e><c><.> and you are returned to the server prompt.</p> <p>Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1B.</p> |
| <p>12. <input type="checkbox"/></p> | <p>Virtual PMAC: Initialize</p> | <p>Initialize switch1B by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml l Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</pre> <p>Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined..</p> <p>A successful completion of netConfig returns you to the prompt.</p> <p>Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname Hostname: switch1B</pre> |
| <p>13. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify IOS image</p> | <p>Verify the switch is using the proper IOS image per Platform version by issuing the following commands:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> |

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---------------------------------|--|--|
| 14. <input type="checkbox"/> | Virtual PMAC: Disable TFTP | <p>Modify PMAC Feature to disable TFTP.</p> <p>Disable the DEVICE.NETWORK.NETBOOT feature.</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm editFeature -- featureName=DEVICE.NETWORK.NETBOOT --enable=0 \$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures</pre> <p>Note: This may take up to 60 seconds to complete.</p> |
| 15. <input type="checkbox"/> | Virtual PMAC: Configure both switches | <p>Configure both switches by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml Processing file: /usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml</pre> <p>Note: This may take up to 2-3 minutes to complete.</p> <p>Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns the user to the prompt.</p> |
| 16. <input type="checkbox"/> | Management Server: Ensure interface are enabled on the TVOE host | <p>Press Ctrl-J to exit the virtual PMAC console. This returns the terminal to the server prompt.</p> <p>Ensure the interfaces of the server connected to switch1A and switch1B are up by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifup <ethernet_interface_2></pre> |
| 17. <input type="checkbox"/> | Cabinet: Connect cables from customer network | <p>Attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.</p> <p>Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.</p> |
| 18. <input type="checkbox"/> | Virtual PMAC: Verify access to customer network | <p>Verify connectivity to the customer network by issuing the following command:</p> <pre>\$ /bin/ping <customer_supplied_ntp_server_address> PING ntpserver1 (10.250.32.51) 56(84) bytes of data. 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms</pre> |
| 19. <input type="checkbox"/> | Cabinet: Connect cables from customer network | <p>Attach switch1B customer uplink cables and detach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports.</p> <p>Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.</p> |

Procedure 2. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---------------------------------|--|---|
| 20. <input type="checkbox"/> | Virtual PMAC: Verify access to customer network | Verify connectivity to the customer network by issuing the following command: <pre>\$ /bin/ping <customer_supplied_ntp_server_address> PING ntpserver1 (10.250.32.51) 56(84) bytes of data. 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms</pre> |
| 21. <input type="checkbox"/> | Cabinet: Connect cables from customer network | Re-attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active. |
| 22. <input type="checkbox"/> | Management Server: Restore the TVOE host back to its original state | Press Ctrl-] to exit the virtual PMAC console. This returns the terminal to the server prompt. Restore the server networking back to original state: <pre>\$ sudo /sbin/service network restart</pre> |
| 23. <input type="checkbox"/> | Back up switch and/or enclosure switch | Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) for each switch configured in this procedure. |

3.2.2 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (RMS System, No PMAC Installed) (netConfig)

This procedure configures 4948/4948E/4948E-F switches with an appropriate IOS and configuration from two management servers for use with the rack mount server platform.

This procedure assumes a Platform 7.6.x interconnect. If the system being configured follows a different platform interconnect, then follow the appropriate platform procedures.

Prerequisites:

- 3.1 Configure netConfig Repository
- 8.1 IPM Management Server
- Application management network interfaces must be configured on the management servers before executing this procedure.
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.
- netConfig is installed

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate value from [2] HP Solutions Firmware Upgrade Pack.

| Variable | Cisco 4948 | Cisco 4948E | Cisco 4948E-F |
|------------------|------------|-------------|---------------|
| <IOS_image_file> | | | |

Fill in the appropriate value for this site.

| Variable | Value |
|---|--------|
| <switch_platform_username> See referring application documentation | |
| <switch_platform_password> | |
| <switch_console_password> | |
| <switch_enable_password> | |
| <mgmt._network> The management network in CIDR format | |
| <management_server_mgmt_IP_address> | |
| <pmac_mgmt_IP_address> | |
| <switch_mgmtVLAN_ID> | |
| <switch1A_mgmtVLAN_IP_address> | |
| <mgmt_Vlan_subnet_ID> | |
| <netmask> | |
| <switch1B_mgmtVLAN_IP_address> | |
| <switch_Internal_VLAN_list> | |
| <management_server_mgmtInterface> | |
| <management_server_iLO_IP> | |
| <customer_supplied_ntp_server_address> | |
| <platcfg_password> Initial password as provided by Oracle | |
| <management_server_mgmtInterface> Value gathered from NAPD | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> Check application documentation | |

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Uplinks must be disconnected from the customer network before executing this procedure. One of the steps in this procedure instructs when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.
- Filenames and sample command line input/output throughout this procedure do not specifically reference the 4948E-F. Template settings are identical between the 4948E and 4948E-F. The original 4948 switch – as opposed to the 4948E or the 4948E-F is referred to simply by the model number 4948. Where all three switches are referred to, this is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Virtual PMAC: Verify IOS image is on the system | Determine if the IOS image for the 4948/4948E/4948E-F is on the PMAC. <pre>\$ /bin/ls -i /var/TKLC/smac/image/<IOS_image_file></pre> If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes. |
| 2. <input type="checkbox"/> | Management Server: Enable tftp on the system for tftp transfer of IOS upgrade file | <pre>\$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp Login on Remote: platcfg Password of platcfg: <platcfg_password> 1 \$ sudo iptablesAdm insert --type=rule --protocol=ipv4 -- domain=10platnet -- table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp -- dport 69 -j ACCEPT" --location=1</pre> |
| 3. <input type="checkbox"/> | Management Server: Verify firewall is configured | <pre>\$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter Persist_Domain__Table_Chain_Match Yes 10platnet filter INPUT -s <mgmt_network> -p udp -dport 69 -j ACCEPT</pre> |

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|--|---|--|
| <p>4. <input type="checkbox"/></p> | <p>Management Server: Manipulate host server physical interfaces</p> | <p>Ensure the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address></p> <pre>\$ sudo /usr/bin/virsh console vm-pmac1A</pre> <p>Note: On a TVOE host, if you open the virsh console, i.e., <code>\$ sudo virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or output is not correct, then more than likely there is a stuck virsh console command already being run on the TVOE host. Exit the virsh console, and run <code>ps -ef grep virsh</code>, then kill the existing process <code>\$ sudo kill -9 <PID></code>. Execute the <code>\$ sudo virsh console X</code> command again. Your console session should now run as expected.</p> |
| <p>5. <input type="checkbox"/></p> | <p>Management Server: Determine if switch1A PROM upgrade is required</p> | <p>Note: ROM and PROM are intended to have the same meaning for this procedure.</p> <p>Connect to switch1A and check the PROM version. Connect serially to switch1A by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter `^Ec?' for help] Press Enter Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> <p>Note: If the console command fails, contact Error! Bookmark not defined..</p> <p>Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing <Ctrl-e><c><. > and you are returned to the server prompt.</p> <p>Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.</p> |

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|--|---|---|
| <p>6. <input type="checkbox"/></p> | <p>Management Server: Verify the initialization template xml files care the correct versions</p> | <p>Verify the initialization template xml files are in existence on the management server and are the correct versions for the system. If no template file is present, copy the files from application media.</p> <ol style="list-style-type: none"> Verify the initialization xml template files and configuration xml template file are present on the system. <pre>\$ sudo /bin/more /usr/TKLC/plat/etc/switch/xml/switch1A_4948_4948E_init.xml \$ sudo /bin/more /usr/TKLC/plat/etc/switch/xml/switch1B_4948_4948E_init.xml \$ sudo /bin/more /usr/TKLC/plat/etc/switch/xml/4948_4948E_configure.xml</pre> <p>If the files do not exist, copy the files onto the management server from the application media using application provided procedures.</p> Verify the xml template files are of the correct version for the system. Ensure the version reported in the following command matches the apiVersion reported in the <configure apiVersion="x.y"> tag at the beginning of each file. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --showVersion API version: 1.1</pre> |
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Modify switch1A_4948_4948E.xml and switch1B_4948_4948E.xml</p> | <p>Modify switch1A_4948_4948E_init.xml and switch1B_4948_4948E_init.xml files for information needed to initialize the switch.</p> <p>Update the init.xml files for all values preceded by a dollar sign. For example, if a value has <code>\$some_variable_name</code>, that value is modified and the dollar sign must be removed during the modification.</p> <p>When done editing the file, save and exit to return to the command prompt.</p> |
| <p>8. <input type="checkbox"/></p> | <p>Virtual PMAC: Modify 4948E-F_configure.xml</p> | <p>Modify 4948E-F_configure.xml for information needed to configure the switches.</p> <p>Update the configure.xml file for all values preceded by a dollar sign. For example, if a value has <code>\$some_variable_name</code>, that value is modified and the dollar sign must be removed during the modification.</p> <p>When done editing the file, save and exit to return to the command prompt.</p> <p>Note: For IPv6 Configurations, IPv6 over NTP is NOT currently supported on the Cisco 4948E-F aggregation switches. This function must be configured for IPv4.</p> |

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---|---|---|
| <p>9. <input type="checkbox"/></p> | <p>Virtual PMAC: Initialize</p> | <p>Initialize switch1A by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml l</pre> <p>Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</p> <p>Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns you to the prompt.</p> <p>Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname</pre> <p>Hostname: switch1A</p> <p>Note: If this command fails, stop this procedure and contact Error! Bookmark not defined.</p> |
| <p>10. <input type="checkbox"/></p> | <p>Management Server: Verify IOS image</p> | <p>Verify the switch is using the proper IOS image per Platform version by issuing the following commands:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware</pre> <p>Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</p> |
| <p>11. <input type="checkbox"/></p> | <p>Management Server: Manipulate host server physical interfaces</p> | <p>Ensure the interface of the server connected to switch1B is the only interface up and obtain the IP address of the management server management interface by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>.</p> |

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---|---|---|
| <p>12. <input type="checkbox"/></p> | <p>Management Server: Determine if switch1B PROM upgrade is required</p> | <p>Note: ROM AND PROM are intended to have the same meaning for this procedure.</p> <p>Connect to switch1A and check the PROM version. Connect serially to switch1A by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter `^Ec?' for help] Press Enter Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> <p>Note: If the console command fails, contact Error! Bookmark not defined..</p> <p>Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing <Ctrl-e><c><. > and you are returned to the server prompt.</p> <p>Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1B.</p> |
| <p>13. <input type="checkbox"/></p> | <p>Virtual PMAC: Initialize</p> | <p>Initialize switch1B by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml l Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</pre> <p>Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined..</p> <p>A successful completion of netConfig returns you to the prompt.</p> <p>Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname Hostname: switch1B</pre> |
| <p>14. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify IOS image</p> | <p>Verify the switch is using the proper IOS image per Platform version by issuing the following commands:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> |

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---------------------------------|--|--|
| 15. <input type="checkbox"/> | Virtual PMAC: Validate XML file | This script validates the XML file to a limited extent. It verifies: <ul style="list-style-type: none"> • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values To validate the XML file: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig - file=4948_4948E_configure.xml -testRun > dev/null</pre> If nothing is returned then the XML file is valid to the extent defined above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file. |
| 16. <input type="checkbox"/> | Virtual PMAC: Configure the switches | Configure both switches by issuing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml Processing file: /usr/TKLC/smac/etc/switch/xml/4948_4948E_configure.xml</pre> <p>Note: This may take up to 2-3 minutes to complete.</p> Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined. A successful completion of netConfig returns the user to the prompt. |
| 17. <input type="checkbox"/> | Management Server: Ensure interface are enabled on the TVOE host | Press Ctrl-] to exit the virtual PMAC console. This returns the terminal to the server prompt. Ensure the interfaces of the server connected to switch1A and switch1B are up by performing the following commands: <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifup <ethernet_interface_2></pre> |
| 18. <input type="checkbox"/> | Cabinet: Connect cables from customer network | Attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. <p>Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.</p> |
| 19. <input type="checkbox"/> | Virtual PMAC: Verify access to customer network | Verify connectivity to the customer network by issuing the following command: <pre>\$ /bin/ping <customer_supplied_ntp_server_address> PING ntpserver1 (10.250.32.51) 56(84) bytes of data. 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms</pre> |

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---------------------------------|---|--|
| 20. <input type="checkbox"/> | Cabinet: Connect cables from customer network | Attach switch1B customer uplink cables and detach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active. |
| 21. <input type="checkbox"/> | Virtual PMAC: Verify access to customer network | Verify connectivity to the customer network by issuing the following command: <pre>\$ /bin/ping <customer_supplied_ntp_server_address> PING ntpserver1 (10.250.32.51) 56(84) bytes of data. 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms</pre> |
| 22. <input type="checkbox"/> | Cabinet: Connect cables from customer network | Re-attach switch1A customer uplink cables. Refer to application documentation for which ports are uplink ports. Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active. |
| 23. <input type="checkbox"/> | Management Server: Restore the TVOE host back to its original state | Press Ctrl-J to exit the virtual PMAC console. This returns the terminal to the server prompt. Restore the server networking back to original state: <pre>\$ sudo /sbin/service network restart</pre> |
| 24. <input type="checkbox"/> | Management Server: Disable TFTP | <pre>\$ sudo /usr/TKLC/plat/bin/tpdProv d --client --noxml --ns=Xinetd stopXinetdService service tftp force yes</pre> Login on Remote: platcfg Password of platcfg: <platcfg_password> 1 Ensure the tftp service is not running by executing the following command. A zero is expected. <pre>\$ sudo /usr/TKLC/plat/bin/tpdProv d --client --noxml --ns=Xinetd getXinetdService service tftp</pre> Login on Remote: platcfg Password of platcfg: <platcfg_password> 0 If a 1 is returned, repeat this step until getXinetdService returns a zero. |
| 25. <input type="checkbox"/> | Management Server: Remove the iptables rule to allow TFTP | <pre>\$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp --dport 69 -j ACCEPT"</pre> |

Procedure 3. Configure Cisco 4948/4948E/4948E-F Aggregation Switches

| Step | Procedure | Result |
|---------------------------------|---|--|
| 26. <input type="checkbox"/> | Management Server: Verify the firewall is configured properly | <pre>\$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter Persist_Domain ___ Table ___ Chain Match</pre> |
| 27. <input type="checkbox"/> | Back up switch and/or enclosure switch | Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) for each switch configured in this procedure. |

3.2.3 Configure Cisco 9372TX-E Aggregation Switches (PMAC Installed) (netConfig)

This procedure configures Cisco 9372TX-E switches to be used in a 10GE-RMS deployment. This procedure also includes how to configure the netConfig repository for all required services and switch information.

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC

At any time, you can view the contents of the netConfig repository by executing one of the following commands on the netConfig Server:

- For switches, use the command:

```
sudo /usr/TKLC/plat/bin/netConfig --repo listDevices
```
- For services, use the command:

```
sudo /usr/TKLC/plat/bin/netConfig --repo listServices
```

Users returning to this procedure after initial installation should run the above commands and note any devices and/or services that have already been configured. Duplicate entries cannot be added; if changes to a device repository entry are required, use the editDevice command. If changes to a services repository entry are necessary, you must delete the original entry first and then add the service again.

IPv4 and IPv6

Platform now supports configuration using IPv4 or IPv6 addresses through netConfig. Wherever IP addresses are required for networking procedures in section 3.1, IPv4 or IPv6 may be used. Commands such as ping or ssh may also be used in these procedures, where for IPv6 cases may need to be ping6 or ssh -6 as needed.

Terminology

The term **netConfig server** refers to the entity where netConfig is executed. This may be a virtualized or physical environment. **Management server** may also accurately describe this location, but has been historically used to describe the physical environment, while **Virtual PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments allow for future simplification of network configuration procedures.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate values.

| Variable | Value |
|---|---------|
| <management_server_iLO_IP> | |
| <management_server_mgmt_IP_address> | |
| <netConfig_server_mgmt_IP_address> | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> See application documentation | |
| <switch_backup_user_home_directory> /usr/TKLC/smac/etc/switch/backup | |
| <platcfg_username> | platcfg |
| <platcfg_password> See application documentation | |
| <frame IDs> List (comma and dash separated values) of frames to be added: Valid frame IDs are 1-7 | |
| <switch IDs> List (comma and dash separated values) of frames to be added: Valid frame IDs are A-F | |
| <json file> JSON file or list of files that define the switch configuration(s) | |

The following table should be filled out using information for the first Cisco 9372TX-E switch. The table should be repeated for each switch to be configured at this site:

| Variable | Value |
|--|-------|
| <switch_hostname> | |
| <switch_username> | |
| <switch_password> | |
| <switch_mgmt_IP_address> CIDR format | |
| <switch_oobm_IP> CIDR format – IPv4 is required | |
| <mgmt_VLAN_ID> | |
| <control_VLAN_ID> | |
| <oobm_VLAN_ID> For switch Frame 1 ID A and Frame 1 ID B the oobm_vlanID should be 1 | |

| Variable | Value |
|--|-------|
| <customer_oam_uplink> See NAPD or Site Survey information. This should be the switchport or LAG that connects to the customers OAM network. | |
| <fw_filename> The firmware version must match the operational redundant switch. This is checked in a procedural step. | |
| <ssh_service> ssh_service to be used for firmware transfer | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Management Server iLO: Login | Log into the management server iLO on the remote console using application provided passwords via Appendix E. Note: If executing this procedure to add switches/frames after the initial deployment (that is, a second pass to add hardware to an existing deployment), the virtual PMAC can be accessed directly via SSH instead of iLO and steps 1 and 2 may be skipped. |

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

| Step | Procedure | Result |
|--|--|---|
| <p>2. <input type="checkbox"/></p> | <p>Management Server: Pre-check</p> | <p>1. Verify virtual PMAC installation by issuing the following commands as admusr on the management server:</p> <pre>\$ sudo /usr/bin/virsh list --all</pre> <pre>Id Name State --- - 6 vm-pmac1A running</pre> <p>Note: If this command provides no output, it is likely that a virtual instance of PMAC is not installed. If there is a virtual PMAC, log into the console of the virtual PMAC.</p> <p>2. From the management server, log into the console of the virtual PMAC instance found above.</p> <p>Example:</p> <pre>\$ sudo /usr/bin/virsh console vm-pmac1A Connected to domain vm-pmac1A Escape character is ^] <Press ENTER key> CentOS release 6.2 (Final) Kernel 2.6.32-220.7.1.el6prere16.0.0_80.13.0.x86_64 on an x86_64</pre> <p>Note: On a TVOE host, if you open the virsh console, i.e., <code>\$ sudo virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or output is not correct, then more than likely there is a stuck virsh console command already being run on the TVOE host. Exit the virsh console, and run <code>ps -ef grep virsh</code>, then kill the existing process <code>\$ sudo kill -9 <PID></code>. Execute the <code>\$ sudo virsh console X</code> command again. Your console session should now run as expected.</p> <p>If the root user is already logged in, log out and log back in as admusr.</p> <pre>[root@pmac ~]# logout vm-pmac1A login: admusr Password: Last login: Fri May 25 16:39:04 on ttyS4</pre> |
| <p>3. <input type="checkbox"/></p> | <p>netConfig Repository: Configure the netConfig repository</p> | <p>Execute the configureRepo utility to configure the netConfig repository. Answer the prompts using the information collected in tables above. Values in square brackets [value] are default values. To use the default value, press Enter at the prompt. Values in BOLD> are entered by the user.</p> <p>Note: Multiple switches can be added at the same time by using a dash or comma(s) (for example, <code>configureRepo --switchID A-B --frameID 1-2</code> or <code>configureRepo --switchID A,C,F --frameID 1</code>).</p> <pre>\$ sudo /usr/TKLC/plat/bin/configureRepo --switchID <switch IDs> - -frameID <frame IDs> What topology should the repository be configured for (ex. 10GE- RMS, topol, etc.)? [10GE-RMS]: Would you like to add a(n) ssh service? [Y/N]: y What is the name of the SSH service? ssh_service What is the IP address of the SSH service?</pre> |

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

| Step | Procedure | Result |
|------|-----------|--|
| | | <pre> <netConfig_server_mgmt_ip_address> What is the username for the SSH service? <switch_backup_user> What is the password for the SSH service? <switch_backup_user_password> Would you like to add another ssh service? [Y/N] n Would you like to add a(n) tftp service? [Y/N]: n Would you like to add a(n) console service? [Y/N]: n Would you like to add a(n) oa service? [Y/N]: n Note: The following prompts repeat for each FrameID-SwitchID combination to be added. Only one set of prompts is provided as an example of tool execution. Adding Frame 1 Switch A (F1-A) What type of switch should be added for F1-A? [C9372TX-E]: What is the name of switch F1-A? <switch_hostname> What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management? <switch_mgmt_ip_address> What is the switchport mode (access trunk) for the management server port? [trunk]: Is the management interface a port or a vlan? [vlan]: What is the VLAN ID of the management VLAN? [2]: <mgmt_vlanID> What is the name of the management VLAN? [management]: What are the allowed vlans for the management server port? [1-2]: <control_vlanID>,<mgmt_vlanID> What switchport connects to the management server? [tenGE1]: What switchport is used as the customer OAM uplink? [fortyGE3]: What is the device username? <switch_username> What is the device password? <switch_password> What is the OOBM IP address (CIDR notation)? <switch_oobm_IP> Enter the name of the firmware file [nxos.7.0.3.I4.2.bin]: <fw_filename> Enter the name of the ssh_service to use for firmware transfers: <ssh_service> Enter the directory for file transfers [/home/admsusr]: <switch_backup_user_home_directory> What is the OOBM VLAN ID? [1]: <oobm_vlanID> Repo Setup Complete. </pre> |

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

| Step | Procedure | Result |
|--|--|---|
| <p>4. <input type="checkbox"/></p> | <p>netConfig Server: Verify FW file is in correct location with correct permissions</p> | <p>For Cisco 9327TX-E switches, the firmware file is large and should be copied to the /var/TKLC/upgrade directory to prevent inadvertently filling up the / or /home partitions on the PMAC.</p> <pre>\$ ls -al /var/TKLC/upgrade/<fw_filename> -rw-r--r-- 1 root root 613 Mar 30 12:31 <fw_filename></pre> <p>If the FW file does not exist, copy the file onto the virtual PMAC.</p> <p>To ensure permissions of the file are correct, execute the following command:</p> <pre>\$ sudo /bin/chmod 644 /var/TKLC/upgrade/<fw_filename></pre> <p>Execute the following command to confirm the new permissions:</p> <pre>\$ ls -al /var/TKLC/upgrade/<fw_filename> -rw-r--r-- 1 root root 696987648 Mar 30 12:31 <fw_filename></pre> <p>Execute the following command to verify the <switch_backup_user> directory has a symbolic link to the FW file in /var/TKLC/upgrade:</p> <pre>\$ ls -al ~<switch_backup_user>/<fw_filename> lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> -> /var/TKLC/upgrade/<fw_filename></pre> <p>If the symbolic link does not exist, execute the following series of commands to create the link and verify it was created correctly:</p> <pre>\$ cd ~<switch_backup_user> \$ ln -s /var/TKLC/upgrade/<fw_filename> \$ ls -al ~<switch_backup_user>/<fw_filename> lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> -> /var/TKLC/upgrade/<fw_filename></pre> |
| <p>5. <input type="checkbox"/></p> | <p>netConfig Server: Verify JSON file exists and modify with site information</p> | <p>1. Verify the configuration JSON file is present on the system and is the correct version for the system.</p> <pre>\$ sudo /bin/more /usr/TKLC/smac/etc/switch/<json_file></pre> <p>If the file does not exist, copy the file onto the virtual PMAC from the application media using application provided procedures.</p> <p>2. Modify the JSON file(s) with necessary site information</p> |
| <p>6. <input type="checkbox"/></p> | <p>netConfig Server: Initialize and configure the switches</p> | <p>The configureSwitch utility allows initialization/configuration of one or many switches with a single execution. If desired, run this utility for each switch one at a time rather than all at once. If that is the case, this step should be repeated for each switch. Alternatively, multiple switches can be added at the same time by using a dash or commas (for example, configureRepo --switchID A-B --frameID 1-3 or configureRepo --switchID A,C,E --frameID 1).</p> <pre>\$ sudo /usr/TKLC/plat/bin/configureSwitch --frameID <frame IDs> - -switchID <switch IDs> --file /usr/TKLC/smac/etc/switch/<json_file> -v</pre> <p>Enter your platcfg username, followed by [ENTER]: <platcfg_username></p> <p>Enter your platcfg password, followed by [ENTER]: <platcfg_password></p> |

Procedure 4. Configure Cisco 9372TX-E Aggregation Switches

| Step | Procedure | Result |
|--|---|--|
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify firmware update</p> | <p>Verify if a final reboot is needed by making sure the firmware and system versions on the switch match. Execute the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getVersion</pre> <p>The following example shows where the System and Firmware versions on the switch do not match and a final reboot is needed:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getVersion Firmware Version: 7.0(3)I4(2) System Version: 7.0(3)I4(5) BIOS Version: 07.51</pre> <p>If the system and firmware versions do not match, reboot the switch, wait until it reboots, and recheck the firmware versions. Execute the following commands to reboot the switch, confirm it is ready to proceed (via ping), and recheck the versions:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> reboot \$ /bin/ping -w 3 <switch_IP> \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> getVersion Firmware Version: 7.0(3)I4(2) System Version: 7.0(3)I4(2) BIOS Version: 07.51</pre> <p>Repeat this step for each switch configured with configureSwitch.</p> |
| <p>8. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify proper configuration of switches</p> | <p>Verify network reachability and configuration.</p> <pre>\$ /bin/ping -w3 <switch_IP> \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> showConfiguration</pre> <p>Inspect the output of showConfiguration and ensure it is configured as per site requirements.</p> <p>It is important to note that the output of showConfiguration provides data in vendor-specific syntax/language. The user should specifically look for the existence of expected VLANs and IP addresses to verify the configuration is correct.</p> |
| <p>9. <input type="checkbox"/></p> | <p>Back up HP for each switch</p> | <p>Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure.</p> |

3.2.4 Replace a Failed 4948/4948E/4948E-F Switch (PMAC Installed) (netConfig)

This procedure replaces a failed 4948/4948E/4948E-F switch.

This procedure assumes a PMAC 6.6 interconnect. If the system being configured follows a different platform interconnect, then the appropriate platform procedures should be followed.

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC
- A fully configured and operational redundant switch must be in operation. If this is not ensured, connectivity may be lost to the end devices.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate value from [2] HP Solutions Firmware Upgrade Pack.

| Variable | Cisco 4948 | Cisco 4948E | Cisco 4948E-F |
|-------------------|------------|-------------|---------------|
| <PROM_image_file> | | | |
| <IOS_image_file> | | | |

Fill in the appropriate value for this site.

| Variable | Value |
|--|--------|
| <switch_console_password> See referring application documentation | |
| <switch_enable_password> See referring application documentation | |
| <management_server_mgmt_IP_address> | |
| <switch1A_mgmtVLAN_IP_address> | |
| <switch1B_mgmtVLAN_IP_address> | |
| <switch_mgmtVLAN_ID> | |
| <management_server_mgmtInterface> | |
| <management_server_iLO_IP> | |
| <netmask> | |
| <mgmt_VLAN_ID> Value gathered from NAPD | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> Check application documentation | |

| Ethernet Interface | DL 360 | DL 380 | X3-2 | X5-2 and X6-2 | X7-2 |
|------------------------|--------|--------|-------|---------------|-------|
| <ethernet_interface_1> | eth01 | eth01 | eth01 | eth01 | eth02 |
| <ethernet_interface_2> | eth02 | eth02 | eth02 | eth03 | eth03 |

| Variable | Platform 7.6.x |
|--------------------------------|----------------|
| <management_server_switchport> | gi1/40 |

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Filenames and sample command line input/output throughout this procedure do not specifically reference the 4948E-F. Template settings are identical between the 4948E and 4948E-F. The original 4948 switch – as opposed to the 4948E or the 4948E-F is referred to simply by the model number 4948. Where all three switches are referred to, this is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Cabinet: Power off failed switch | If the failed switch is DC powered, power off using the cabinet breakers, then remove the DC power and ground cables. If the failed switch is AC powered, remove the AC power cords from the unit. |
| 2. <input type="checkbox"/> | Cabinet: Find and prepare to replace switch | Determine whether switch1A or switch1B failed, locate the failed switch, and detach all network and console cables from the failed switch. Note: If needed label cables before removal. |
| 3. <input type="checkbox"/> | Cabinet: Replace switch | Remove failed switch and replace with new switch of same model. |
| 4. <input type="checkbox"/> | Cabinet: Power on replacement switch | If the switch is DC powered, attach the DC power and ground cables, then power on the replacement switch using the appropriate cabinet breakers; otherwise, connect the AC power cords to the unit (AC). |
| 5. <input type="checkbox"/> | Cabinet: Attach cable to new switch | Connect all network and console cables to the new switch except the customer uplink cables. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch. Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink. |

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|-----------------|---|--|
| <p>6. □</p> | <p>Virtual PMAC: Verify IOS image is on system</p> | <p>If the appropriate image does not exist, copy the image to the PMAC. Note: Check the FW version on the mate switch and select the matching FW image from the backup directory/TFTP directory.</p> <p>To check the FW on the mate switch, use the following command: If replacing switch1A: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware</pre> </p> <p>If replacing switch1B: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware</pre> </p> <pre>Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> <p>Determine if the IOS image for the 4948/4948E/4948E-F is on the virtual PMAC. <pre>\$ sudo /bin/ls -l /var/TKLC/smac/image/<IOS_image_file> \$ sudo /bin/ls -l <switch_backup_directory>/<ios_image></pre> </p> <p>If the file exists and is in the TFTP directory, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media. If the file is in the backup directory copy it to the TFTP directory: <pre>\$ sudo /bin/cp -i <switch_backup_directory>/<ios_image> /var/TKLC/smac/image/</pre> </p> |
| <p>7. □</p> | <p>Virtual PMAC: Modify PMAC feature to allow TFTP</p> | <p>Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm editFeature -- featureName=DEVICE.NETWORK.NETBOOT --enable=1 \$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures</pre> </p> <p>This may take up to 60 seconds to complete.</p> |

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|-----------------|---|---|
| <p>8. □</p> | <p>Management Server: Manipulate host server physical interfaces</p> | <p>Exit from the virtual PMAC console, by pressing Ctrl-] and you are returned to the server prompt.</p> <p>Ensure the interface of the server connected to switch1A is the only interface up and obtain the IP address of the management server management interface by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>.</p> <pre>\$ sudo /usr/bin/virsh console vm-pmac1A</pre> <p>Note: On a TVOE host, if you open the virsh console, i.e., <code>\$ sudo virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or output is not correct, then more than likely there is a stuck virsh console command already being run on the TVOE host. Exit the virsh console, and run <code>ps -ef grep virsh</code>, then kill the existing process <code>\$ sudo kill -9 <PID></code>. Execute the <code>\$ sudo virsh console X</code> command again. Your console session should now run as expected.</p> |

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|---|--|---|
| <p>9. <input type="checkbox"/></p> | <p>Management Server: Get PROM information</p> | <p>Note: ROM and PROM are intended to have the same meaning for this procedure.</p> <p>Connect to switch and check the PROM version.</p> <p>If replacing switch1A:</p> <p>Connect serially to switch1A by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console</pre> <p>If replacing switch1B:</p> <p>Connect serially to switch1B by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1B_console</pre> <pre>Enter platcfg@pmac5000101's password: <platcfg_password> [Enter '^Ec?' for help] Press Enter Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> <p>Note: If the console command fails, contact Error! Bookmark not defined.</p> <p>Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing <Ctrl-e><c><. > and you are returned to the server prompt.</p> <p>Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.</p> |
| <p>10. <input type="checkbox"/></p> | <p>Virtual PMAC: Reset switch to factory defaults</p> | <p>Connect serially to the switch and reload the switch by issuing the following commands:</p> <pre>Switch# write erase Switch reload</pre> <p>Wait until the switch reloads, then exit from console; press <Ctrl-e><c><. > and you are returned to the server prompt. Wait for the first switch to finish before repeating this process for the second switch.</p> <p>Note: There might be messages from the switch. If asked to confirm, press Enter. If asked yes or no, type in no and press Enter.</p> |

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|------------------|---|---|
| <p>11. □</p> | <p>Virtual PMAC: Initialize switch</p> | <p>Older platform init files may not work on Platform 7.6.x systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy switch1A_4948_4948E_init.xml.</p> <p>If replacing switch1A, issue the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</pre> <p>If replacing switch1B, issue the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml</pre> <p>Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</p> <p>Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns you to the prompt.</p> <p>Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.</p> <p>For switch1A:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname Hostname: switch1A</pre> <p>For switch1B:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname Hostname: switch1B</pre> |
| <p>12. □</p> | <p>Virtual PMAC: Verify IOS image</p> | <p>Verify the switch is using the proper IOS image per Platform version by issuing the following commands:</p> <p>For switch1A:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware</pre> <p>For switch1B:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware</pre> <pre>Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> |

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|---------------------------------|--|---|
| 13. <input type="checkbox"/> | Virtual PMAC: Copy the switch backup files to the current directory | <pre>\$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<swname>- backup ~<switch_backup_user>/ \$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<swname>- backup.info ~<switch_backup_user>/</pre> <p>Get a list of the file copied over.</p> <p>Note: switch1A is shown as an example.</p> <pre>\$ /bin/ls -l switch1A-backup switch1A-backup.info</pre> |
| 14. <input type="checkbox"/> | Virtual PMAC: Restore | <pre>\$ cd ~<switch_backup_user> \$ sudo /bin/chmod 644 ~<switch_backup_user>/<swname>-backup* \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> restoreConfiguration service=ssh_service filename=<swname>- backup</pre> <p>Note: If the command failed with error message same as or similar to Error saving to service, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to Appendix T.</p> |
| 15. <input type="checkbox"/> | Virtual PMAC: Make sure both interfaces are enabled on the TVOE host | <p>Connect to the TVOE host and ensure the interfaces of the server connected to switch1A and switch1B are up by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifup <ethernet_interface_2></pre> |
| 16. <input type="checkbox"/> | Virtual PMAC: Verify switch configuration | <p>Ping each of the switches' SVI (router interface) addresses to verify switch configuration.</p> <pre>\$ /bin/ping <switch1A_mgmtVLAN_IP> \$ /bin/ping <switch1B_mgmtVLAN_IP></pre> |
| 17. <input type="checkbox"/> | Virtual PMAC: Verify switch is using proper IOS image per platform version | <p>To verify the IOS release on each switch:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A listFirmware Image: cat4500-ipbasek9-mz.122-53.SG2.bin \$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B listFirmware Image: cat4500-ipbasek9-mz.122-53.SG2.bin</pre> |
| 18. <input type="checkbox"/> | Cabinet: Connect cables from customer network | <p>Attach customer uplink cables. Refer to application documentation for which ports are uplink ports.</p> <p>Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active.</p> |

Procedure 5. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|---------------------------------|---|---|
| 19. <input type="checkbox"/> | Virtual PMAC: Verify access to customer network | Verify connectivity to the customer network by issuing the following command: <pre>\$ /bin/ping <customer_supplied_ntp_server_address> PING ntpserver1 (10.250.32.51) 56(84) bytes of data. 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms</pre> |
| 20. <input type="checkbox"/> | Virtual PMAC: Clean up FW | Remove the FW images from the users' home directory and TFTP directory with the following command: <pre>\$ sudo rm ~admusr/<fw_filename> \$ sudo rm /var/TKLC/smac/image/<fw_filename></pre> |

3.2.5 Replace a Failed 4948/4948E/4948E-F Switch (RMS System, No PMAC Installed) (netConfig)

This procedure replaces a failed 4948/4948E/4948E-F switch.

This procedure assumes a Platform 7.6.x interconnect. If the system being configured follows a different platform interconnect, then the appropriate platform procedures should be followed.

Prerequisites:

- Complete 8.1 IPM Management Server before this procedure is attempted.
- A fully configured and operational redundant switch must be in operation. If this is not ensured, connectivity may be lost to the end devices.
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate value from [2] HP Solutions Firmware Upgrade Pack.

| Variable | Cisco 4948 | Cisco 4948E | Cisco 4948E-F |
|-------------------|------------|-------------|---------------|
| <PROM_image_file> | | | |
| <IOS_image_file> | | | |

Fill in the appropriate value for this site.

| Variable | Value |
|--|-------|
| <switch_console_password> See referring application documentation | |
| <switch_enable_password> See referring application documentation | |
| <management_server_mgmt_IP_address> | |

| Variable | Value |
|--|--------|
| <switch1A_mgmtVLAN_IP_address> | |
| <switch1B_mgmtVLAN_IP_address> | |
| <switch_mgmtVLAN_ID> | |
| <management_server_iLO_IP> | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> Check application documentation | |

| Ethernet Interface | DL 360 | DL 380 | X3-2 | X5-2 and X6-2 | X7-2 |
|------------------------|--------|--------|-------|---------------|-------|
| <ethernet_interface_1> | eth01 | eth01 | eth01 | eth01 | eth02 |
| <ethernet_interface_2> | eth02 | eth02 | eth02 | eth03 | eth03 |

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.
- Filenames and sample command line input/output throughout this procedure do not specifically reference the 4948E-F. Template settings are identical between the 4948E and 4948E-F. The original 4948 switch – as opposed to the 4948E or the 4948E-F is referred to simply by the model number 4948. Where all three switches are referred to, this is made clear by reference to 4948/4948E/4948E-F switches.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Cabinet: Power off failed switch | If the failed switch is DC powered, power off using the cabinet breakers, then remove the DC power and ground cables. If the failed switch is AC powered, remove the AC power cords from the unit. |
| 2. <input type="checkbox"/> | Cabinet: Find and prepare to replace switch | Determine whether switch1A or switch1B failed, locate the failed switch, and detach all network and console cables from the failed switch. Note: If needed label cables before removal. |
| 3. <input type="checkbox"/> | Cabinet: Replace switch | Remove failed switch and replace with new switch of same model. |

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|--------------------------------|---|---|
| 4. <input type="checkbox"/> | Cabinet: Power on replacement switch | If the switch is DC powered, attach the DC power and ground cables, then power on the replacement switch using the appropriate cabinet breakers; otherwise, connect the AC power cords to the unit (AC). |
| 5. <input type="checkbox"/> | Cabinet: Attach cable to new switch | Connect all network and console cables to the new switch except the customer uplink cables. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch. Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink |
| 6. <input type="checkbox"/> | Management Server: Verify IOS image is on system | If the appropriate image does not exist, copy the image to the management server. Note: Check the FW version on the mate switch and select the matching FW image from the backup directory/TFTP directory. To check the FW on the mate switch, use the following command: If replacing switch1A: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware</pre> If replacing switch1B: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware</pre> <pre>Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> Determine if the IOS image for the 4948/4948E/4948E-F is on the virtual management server C. <pre>\$ sudo /bin/ls -l /var/TKLC/smac/image/<IOS_image_file> \$ sudo /bin/ls -l <switch_backup_directory>/<ios_image></pre> If the file exists and is in the TFTP directory, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media. If the file is in the backup directory copy it to the TFTP directory: <pre>\$ sudo /bin/cp -i <switch_backup_directory>/<ios_image> /var/TKLC/smac/image/</pre> |

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|--------------------------------|---|---|
| 7. <input type="checkbox"/> | Management Server: Enable tftp on the system for tftp transfer of IOS upgrade file | <pre>\$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd startXinetdService service tftp Login on Remote: platcfg Password of platcfg: <platcfg_password> 1 \$ sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp --dport 69 -j ACCEPT" --location=1</pre> |
| 8. <input type="checkbox"/> | Management Server: Verify firewall is configured | <pre>\$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter Persist_Domain__Table__Chain_Match Yes 10platnet filter INPUT -s <mgmt_network> -p udp -dport 69 -j ACCEPT</pre> |
| 9. <input type="checkbox"/> | Management Server: Manipulate host server physical interfaces | <p>Ensure the interface of the server connected to the switch is the only interface up and obtain the IP address of the management server management interface by performing the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address></p> |

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|------------------|---|---|
| <p>10. □</p> | <p>Management Server: Get PROM information</p> | <p>Note: ROM and PROM are intended to have the same meaning for this procedure.</p> <p>Connect to switch and check the PROM version.</p> <p>If replacing switch1A:</p> <p>Connect serially to switch1A by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console</pre> <p>If replacing switch1B:</p> <p>Connect serially to switch1B by issuing the following command.</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1B_console</pre> <pre>Enter platcfg@pmac5000101's password: <platcfg_password> [Enter '^Ec?' for help] Press Enter Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> <p>Note: If the console command fails, contact Error! Bookmark not defined.</p> <p>Note the IOS image and ROM version for comparison in a following step. Exit from the console by pressing <Ctrl-e><c><. > and you are returned to the server prompt.</p> <p>Verify the version from the previous command against the version from the release notes referenced. If the versions are different, perform the procedure in Appendix G to upgrade the PROM for switch1A.</p> |
| <p>11. □</p> | <p>Management Server: Reset switch to factory defaults</p> | <p>Connect serially to the switch and reload the switch by issuing the following commands:</p> <pre>Switch# write erase Switch reload</pre> <p>Wait until the switch reloads, then exit from console; press <Ctrl-e><c><. > and you are returned to the server prompt. Wait for the first switch to finish before repeating this process for the second switch.</p> <p>Note: There might be messages from the switch. If asked to confirm, press Enter. If asked yes or no, type in no and press Enter.</p> |

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|------------------|--|---|
| <p>12. □</p> | <p>Management Server: Initialize switch</p> | <p>Older platform init files may not work on Platform 7.6.x systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy switch1A_4948_4948E_init.xml.</p> <p>If replacing switch1A, issue the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</pre> <p>If replacing switch1B, issue the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml</pre> <p>Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</p> <p>Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns you to the prompt.</p> <p>Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.</p> <p>For switch1A:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname Hostname: switch1A</pre> <p>For switch1B:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname Hostname: switch1B</pre> |
| <p>13. □</p> | <p>Management Server: Verify IOS image</p> | <p>Verify the switch is using the proper IOS image per Platform version by issuing the following commands:</p> <p>For switch1A:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware</pre> <p>For switch1B:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware</pre> <pre>Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> |

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|---|---|---|
| <p>14. <input type="checkbox"/></p> | <p>Management Server: Initialize switch</p> | <p>Older platform init files may not work on Platform 7.6.x systems. Copy the switch appropriate init.xml file from application media using application provided procedures. For example, for switch1A copy switch1A_4948_4948E_init.xml.</p> <p>If replacing switch1A, issue the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</pre> <p>If replacing switch1B, issue the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/switch1B_4948_4948E_init.xml</pre> <p>Processing file: /usr/TKLC/smac/etc/switch/xml/switch1A_4948_4948E_init.xml</p> <p>Note: This step takes about 5-10 minutes to complete. Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns you to the prompt.</p> <p>Use netConfig to get the hostname of the switch, to verify the switch was initialized properly, and to verify netConfig can connect to the switch.</p> <p>For switch1A:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getHostname Hostname: switch1A</pre> <p>For switch1B:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getHostname Hostname: switch1B</pre> |
| <p>15. <input type="checkbox"/></p> | <p>Management Server: Verify switch is using proper IOS image per platform version</p> | <p>Verify the switch is using the proper IOS image per Platform version by issuing the following commands:</p> <p>For switch1A:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A getFirmware</pre> <p>For switch1B:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B getFirmware</pre> <pre>Version: 122-54.XO License: entservicesk9 Flash: cat4500e-entservicesk9-mz.122-54.XO.bin</pre> |

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|---------------------------------|---|---|
| 16. <input type="checkbox"/> | Management Server: Disable TFTP | <pre>\$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp force yes</pre> <p>Login on Remote: platcfg Password of platcfg: <platcfg_password> 1</p> <p>Ensure the tftp service is not running by executing the following command. A zero is expected.</p> <pre>\$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd getXinetdService service tftp</pre> <p>Login on Remote: platcfg Password of platcfg: <platcfg_password> 0</p> <p>If a 1 is returned, repeat this step until getXinetdService returns a zero.</p> |
| 17. <input type="checkbox"/> | Management Server: Remove the iptables rule to allow TFTP | <pre>\$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp --dport 69 -j ACCEPT"</pre> |
| 18. <input type="checkbox"/> | Management Server: Verify the firewall is configured properly | <pre>\$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter</pre> <p><u>Persist Domain ___ Table ___ Chain Match</u></p> |
| 19. <input type="checkbox"/> | Management Server: Copy the switch backup files to the current directory | <pre>\$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<swname>-backup ~<switch_backup_user>/</pre> <pre>\$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<swname>-backup.info ~<switch_backup_user>/</pre> <p>Get a list of the file copied over.</p> <p>Note: switch1A is shown as an example.</p> <pre>\$ /bin/ls -l</pre> <pre>switch1A-backup</pre> <pre>switch1A-backup.info</pre> <pre>switch1A-backup.vlan</pre> |
| 20. <input type="checkbox"/> | Management Server: Restore | <pre>\$ cd ~<switch_backup_user></pre> <pre>\$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> restoreConfiguration service=ssh_service filename=<switch_hostname>-backup</pre> <p>Note: If the command failed with error message same as or similar to Error saving to service, and the TPD version is 7.6.0.0_88.50.0 or later, refer to Error! Reference source not found.</p> |

Procedure 6. Replace a Failed 4948/4948E/4948E-F Switch

| Step | Procedure | Result |
|---------------------------------|--|---|
| 21. <input type="checkbox"/> | Management Server: Verify switch configuration | Ping each of the switches' SVI (router interface) addresses to verify switch configuration. <pre>\$ /bin/ping <switch1A_mgmtVLAN_IP> \$ /bin/ping <switch1B_mgmtVLAN_IP></pre> |
| 22. <input type="checkbox"/> | Management Server: Verify switch is using proper IOS image per platform version | To verify the IOS release on each switch: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1A listFirmware Image: cat4500-ipbasek9-mz.122-53.SG2.bin \$ sudo /usr/TKLC/plat/bin/netConfig --device=switch1B listFirmware Image: cat4500-ipbasek9-mz.122-53.SG2.bin</pre> |
| 23. <input type="checkbox"/> | Cabinet: Connect cables from customer network | Attach customer uplink cables. Refer to application documentation for which ports are uplink ports. Note: If the customer is using standard 802.1D spanning-tree, the links may take up to 50 seconds to become active. |
| 24. <input type="checkbox"/> | Management Server: Verify access to customer network | Verify connectivity to the customer network by issuing the following command: <pre>\$ /bin/ping <customer_supplied_ntp_server_address> PING ntpserver1 (10.250.32.51) 56(84) bytes of data. 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=0 ttl=62 time=0.150 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=1 ttl=62 time=0.223 ms 64 bytes from ntpserver1 (10.250.32.51): icmp_seq=2 ttl=62 time=0.152 ms</pre> |
| 25. <input type="checkbox"/> | Management Server: Clean up FW | Remove the FW images from the users' home directory and TFTP directory with the following command: <pre>\$ sudo rm ~admusr/<fw_filename> \$ sudo rm /var/TKLC/smac/image/<fw_filename></pre> |

3.2.6 Replace a Failed 9372TX-E Switch (PMAC Installed) (netConfig)

This procedure replaces a failed 9372TX-E switch.

This procedure assumes a healthy PMAC with the original netConfig repository intact. If this is not the case and a PMAC disaster recovery needs to be performed, see [7] PMAC Disaster Recovery, Release 6.6.. If a PMAC does not exist and a DR is not possible, disregard this procedure and perform 3.2.3 Configure Cisco 9372TX-E Aggregation Switches (PMAC Installed) (netConfig).

Prerequisites:

- A fully configured and operational redundant switch must be in operation. If this is not ensured, connectivity may be lost to the end devices.
- Access to the switch configuration backup file for the failed switch. This generally resides on the PMAC in directory `/usr/TKLC/smac/etc/switch/backup` and typically has a name format of `<switch_hostname>-backup`. If the file does not exist on the PMAC, work with the local switch administrator to determine if an offloaded copy exists

Terminology

The term **netConfig server** refers to the entity where netConfig is executed. This may be a virtualized or physical environment. **Management server** may also accurately describe this location, but has been historically used to describe the physical environment, while **Virtual PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments allow for future simplification of network configuration procedures.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate values.

| Variable | Value |
|--|--------|
| <switch_backup_user> | admusr |
| <switch_backup_user_password> Check application documentation | |
| <fw_filename> The firmware version must match the operational redundant switch. This is checked in a procedural step. | |
| <switch_backup_user_home_directory> /usr/TKLC/smac/etc/switch/backup | |
| <management_server_mgmtInterface> | |
| <management_server_mgmt_IP_address> | |

| Ethernet Interface | Oracle Server |
|------------------------|---------------|
| <ethernet_interface_1> | eth01 |
| <ethernet_interface_2> | eth03 |

Note: The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.

Needed Material: Cisco FW file acquired through **Error! Bookmark not defined.**

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 7. Replace a Failed 9372TX-E Switch

| Step | Procedure | Result |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Cabinet: Power off failed switch | If the failed switch is DC powered, power off using the cabinet breakers, then remove the DC power and ground cables. If the failed switch is AC powered, remove the AC power cords from the unit. |
| 2. <input type="checkbox"/> | Cabinet: Find and prepare to replace switch | Determine whether switch1A or switch1B failed, locate the failed switch, and detach all network and console cables from the failed switch. Note: If needed label cables before removal. |
| 3. <input type="checkbox"/> | Cabinet: Replace switch | Remove failed switch and replace with new switch of same model. |

Procedure 7. Replace a Failed 9372TX-E Switch

| Step | Procedure | Result |
|--------------------------------|---|---|
| 4. <input type="checkbox"/> | Cabinet: Power on replacement switch | If the switch is DC powered, attach the DC power and ground cables, then power on the replacement switch using the appropriate cabinet breakers; otherwise, connect the AC power cords to the unit (AC). |
| 5. <input type="checkbox"/> | Cabinet: Attach cable to new switch | Connect all network and console cables to the new switch except the customer uplink cables. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch. Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink |
| 6. <input type="checkbox"/> | Virtual PMAC: Verify IOS image is on system | <p>If the appropriate image does not exist, copy the image to the PMAC.</p> <p>Note: Check the FW version on the mate switch and select the matching FW image from the backup directory/TFTP directory. The firmware version must be identical between mating switches.</p> <p>To check the FW on the mate switch, use the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=<mate_switchname> getFirmware Version: 7-0.I4.2 Flash: nxos.7.0.3.I4.bin</pre> <p>Determine if the IOS image for the 9372TX-E is on the virtual PMAC.</p> <pre>\$ sudo /bin/ls -l <switch_backup_directory>/<fw_filename></pre> <p>or</p> <pre>\$ sudo /bin/ls -l /var/TKLC/upgrade/<fw_filename></pre> <p>If the FW file exists, verify a symbolic link exists to the firmware file in the backup user directory by using the following command:</p> <p>If the file is in the backup directory copy it to the TFTP directory:</p> <pre>\$ sudo /bin/ls -al ~<switch_backup_user>/*.bin lrwxrwxrwx 1 root root 37 Dec 16 16:42 nxos.7.0.3.I4.2.bin -> /var/TKLC/upgrade/nxos.7.0.3.I4.2.bin</pre> <p>If the link exists, verify it is correct by verifying the FW file exists in the location pointed to by the link</p> <p>Note: The FW file location pointed to by the link is everything after the "->" in the output of the previous command.</p> <p>The output below is for example only, and is based on the example output given above:</p> <pre>\$ sudo /bin/ls -al /var/TKLC/upgrade/nxos.7.0.3.I4.2.bin -rw-r--r-- 1 admusr admgrp 696987648 Nov 30 13:38 /var/TKLC/upgrade/nxos.7.0.3.I4.2.bin</pre> <p>If the link does not exist, or is incorrect, remove the existing link and create the correct link by executing the following commands:</p> <pre>\$ cd ~<switch_backup_user> \$ sudo /bin/rm -f ~<switch_backup_user>/<name_of_incorrect_link> \$ cd ~<switch_backup_user> \$ ln -s <switch_backup_directory>/<fw_filename></pre> |

Procedure 7. Replace a Failed 9372TX-E Switch

| Step | Procedure | Result |
|--|---|--|
| | | <pre>\$ ls -al ~<switch_backup_user>/<fw_filename> lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> -> /var/TKLC/upgrade/<fw_filename></pre> <p>If the FW image does not exist on the virtual PMAC, copy it to the switch backup directory. Change the FW image file permissions by executing the following command:</p> <pre>\$ sudo /bin/chmod 644 /var/TKLC/upgrade/<fw_filename></pre> <p>Execute the following command to confirm the new permissions:</p> <pre>\$ ls -al /var/TKLC/upgrade/<fw_filename> -rw-r--r-- 1 root root 696987648 Mar 30 12:31 <fw_filename></pre> <p>Verify the <switch_backup_user> directory has a symbolic link to the FW file in /var/TKLC/upgrade.</p> <pre>\$ ls -al ~<switch_backup_user>/<fw_filename> lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> -> /var/TKLC/upgrade/<fw_filename></pre> <p>If the symbolic link does not exist, execute the following commands to create the link and verify it was created correctly:</p> <pre>\$ cd ~<switch_backup_user> \$ ln -s /var/TKLC/upgrade/<fw_filename> \$ ls -al ~<switch_backup_user>/<fw_filename> lrwxrwxrwx 1 admusr admgrp 37 Dec 16 14:18 /home/admusr/<fw_filename> -> /var/TKLC/upgrade/<fw_filename></pre> |
| <p>7. <input type="checkbox"/></p> | <p>Management Server: Manipulate host server physical interfaces</p> | <p>This step only pertains to failed switches in the first frame with a switchID of A or B. In other words, the switches that host the management server interface. If the failed switch has a switchID of C-F or resides in frame 2 or beyond, this step can be ignored and the user may proceed with the next step.</p> <p>Connect to the management server and perform the following commands:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_1> \$ sudo /sbin/ifdown <ethernet_interface_2> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>.</p> <p>If replacing switch with an identity of frameID 1 switchID B:</p> <pre>\$ sudo /sbin/ifup <ethernet_interface_2> \$ sudo /sbin/ifdown <ethernet_interface_1> \$ sudo /sbin/ip addr show <management_server_mgmtInterface> grep inet</pre> <p>The command output should contain the IP address of the variable, <management_server_mgmt_IP_address>.</p> |

Procedure 7. Replace a Failed 9372TX-E Switch

| Step | Procedure | Result |
|---------------------------------|---|--|
| 8. <input type="checkbox"/> | Virtual PMAC: Initialize switch | Initialize the switch by performing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/initializeSwitch --switch <switch_hostname></pre> Enter your platcfg username, followed by [ENTER]: <pre><platcfg_username></pre> Enter your platcfg password, followed by [ENTER]: <pre><platcfg_password></pre> |
| 9. <input type="checkbox"/> | Virtual PMAC: Copy switch backup file | Copy the switch backup files to the home directory of the <switch_backup_user> by performing the following command: <pre>\$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup* ~<switch_backup_user>/</pre> <pre>\$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup.info ~<switch_backup_user>/</pre> |
| 10. <input type="checkbox"/> | Virtual PMAC: Restore | <pre>\$ cd ~<switch_backup_user></pre> <pre>\$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> restoreConfiguration service=ssh_service filename=<switch_hostname>-backup</pre> <p>Note: If the command failed with error message same as or similar to Error saving to service, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to Appendix T.</p> |
| 11. <input type="checkbox"/> | Management Server: Make sure both interfaces are enabled host server | Connect to the management server perform the following commands: <pre>\$ sudo /sbin/ifup <ethernet_interface_1></pre> <pre>\$ sudo /sbin/ifup <ethernet_interface_2></pre> |
| 12. <input type="checkbox"/> | Cabinet: Connect cables from customer network | Attach customer uplink cables. Refer to application documentation for which ports are uplink ports. |
| 13. <input type="checkbox"/> | Virtual PMAC: Verify proper configuration of switches | Verify network reachability and configuration. <pre>\$ /bin/ping -w3 <switch_IP></pre> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> showConfiguration</pre> <p>Inspect the showConfiguration output to ensure it is configured per site requirements.</p> <p>Note the showConfiguration output provides output in vendor-specific syntax/language. Look for the existence of expected VLANs and IP addresses to verify the configuration is correct.</p> |

Procedure 7. Replace a Failed 9372TX-E Switch

| Step | Procedure | Result |
|---------------------------------|---------------------------------------|---|
| 14. <input type="checkbox"/> | Management Server: Clean up FW | Remove the FW images from the users' home directory and TFTP directory with the following command: <pre>\$ sudo rm ~admusr/<fw_filename> \$ sudo rm /var/TKLC/smac/image/<fw_filename></pre> |

3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig)

This procedure backs up the Cisco aggregation and enclosure switches.

Prerequisites for RMS system aggregation switch:

- 8.1 IPM Management Server
- Step 2 of 9.1 Install TVOE on the Management Server to install the IPM DL380 server.
- 9.2 Configure TVOE Network
- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.

Prerequisites for c-Class system aggregation switch (Oracle-provided):

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)

Prerequisites for Cisco 3020 enclosure switch:

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 3.3.1 Configure Cisco 3020 Switch (netConfig)

| Variable | Value |
|--|--------|
| <switch_backup_user> (also needed in switch configuration procedure) | admusr |
| <switch_backup_user_password> (also needed in switch configuration procedure) Check application documentation | |
| <switch_name> Hostname of the switch | |

| Variable | Value |
|---|-------|
| <switch_backup_directory> Non-PMAC System: /usr/TKLC/plat/etc/switch/backup | |
| PMAC System: /usr/TKLC/smac/etc/switch/backup | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 8. Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch

| Step | Result |
|--------------------------------|---|
| 1. <input type="checkbox"/> | <p>Verify switch is initialized correctly and connectivity to the switch by verifying the hostname.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> getHostname Hostname: switch1A</pre> <p>Note: The value beside Hostname should be the same as the <switch_name> variable.</p> |
| 2. <input type="checkbox"/> | <p>Run the netConfig --repo showService name=ssh_service command and look for ssh service.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service Service Name: ssh_service Type: ssh Host: 10.250.62.85 Options: password: C20F7D639AE7E7 user: admusr</pre> <p>In the ssh_service parameters, the value for user: is the value for the variable <switch_backup_user>.</p> |
| 3. <input type="checkbox"/> | <p>Verify existence of the backup directory.</p> <pre>\$ sudo /bin/ls -i <switch_backup_directory></pre> <p>If the output contains:</p> <pre>ls: cannot access <switch_backup_directory>: No such file or directory</pre> <p>Create the directory with:</p> <pre>\$ sudo /bin/mkdir -p <switch_backup_directory></pre> <p>Change directory permissions:</p> <pre>\$ sudo /bin/chmod go+x <switch_backup_directory></pre> <p>If this is a PMAC system, change ownership:</p> <pre>\$ sudo /bin/chown -R pmacd:pmacbackup <switch_backup_directory></pre> |
| 4. <input type="checkbox"/> | <p>Execute the backup command.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup</pre> <p>Note: If the command failed with error message same as or similar to Error saving to service, and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to Appendix T.</p> |

Procedure 8. Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch

| Step | Result |
|---------------------------------|---|
| 8. <input type="checkbox"/> | Save the PMAC backup. The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: /var/TKLC/smac/backup . |
| 9. <input type="checkbox"/> | Save FW files. If a firmware upgrade, switch replacement, or an initial install (which performed a FW upgrade during initialization) was performed, backup the FW image used by performing one of the following commands: If the FW upgrade was performed with TFTP: If on a PMAC system: <pre>\$ sudo /bin/mv -i /var/TKLC/smac/image/<fw_image> <switch_backup_directory>/</pre> If on a non-PMAC system: <pre>\$ sudo /bin/mv -i /var/lib/tftpboot/<fw_image> <switch_backup_directory>/</pre> If the FW upgrade was performed with SCP: <pre>\$ sudo /bin/mv -i ~<switch_backup_user>/<fw_image> <switch_backup_directory>/</pre> Otherwise, proceed to the next step. |
| 10. <input type="checkbox"/> | Repeat steps 1. and 4. through 6. for each switch to be backed up. |

3.2.8 Replace a Failed Telco T5C-24GT

This procedure configures a Telco T5C-24GT switch with an appropriate configuration from its corresponding T1200 server.

This procedure assumes a T1200 server running TPD 6.7 or higher and connected serially to the Telco T5C-24GT switch console port via /dev/ttyUSB1.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate values.

| Variable | Value |
|----------------------------------|-------|
| <T1200_server_RMM_IP> | |
| <T1200_server_RMM_user> | |
| <T1200_server_RMM_user_password> | |
| <T1200_server__password> | |
| <Telco_switch_name> | |
| <Telco_switch_password> | |
| <Telco_switch_Enable_password> | |
| <T5CL3_24_firmware_image_file> | |

| Variable | Value |
|-----------------------------|-------|
| <Remote_customer_target_IP> | |

Notes:

- See the T1200 Solutions Firmware Upgrade Pack (Tekelec part# 909-1618-001) for appropriate T5CL3_24G firmware image.
- The <Remote_customer_target_IP> is identified later in this procedure.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 9. Replace a Failed Telco T5C-24GT

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Telco T5CL3_24G: Power off failed switch | Identify and power down the failed Telco switch. Label and disconnect all cables connected to the Telco switch. Remove the defective Telco switch |
| 2. <input type="checkbox"/> | Telco T5CL3_24G: Replace switch | Install new Telco switch and re-cable all cables, except for uplinks to customer network. Connect power and power on switch. In the ssh_service parameters, the value for user is the value for the variable <switch_backup_user>. |
| 3. <input type="checkbox"/> | Management Server RMM: Login | Log into the Remote Management module (RMM) using Internet Explorer with the <T1200_server_RMM_user> and <T1200_server_RMM_user_password>. <a href="http://<T1200_server_RMM_IP>">http://<T1200_server_RMM_IP> |
| 4. <input type="checkbox"/> | Management Server RMM: Log into the Telco T1200 remote console | Click the Console icon in the upper left corner to launch the Remote Console on the server. Click Don't Block if the Security Warning window displays. Note: Different versions of Internet Explorer may present additional security prompts. If not already done, login as admusr using the <T1200_server_password> password. |
| 5. <input type="checkbox"/> | Management Server: Verify console connection | Determine whether needed minicom files are already available by issuing the following command: <pre>\$ /bin/ls -l /etc/minirc.*</pre> If the minirc.<Telco_switch_name> file is not listed, set up the serial connections to the switch by issuing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/remoteConsole --add --name=<Telco_switch_name> --bps=9600 --port=ttyUSB1</pre> |

Procedure 9. Replace a Failed Telco T5C-24GT

| Step | Procedure | Result |
|--|--|---|
| <p>6. <input type="checkbox"/></p> | <p>Management Server: Connect serially to the switch</p> | <pre>\$ sudo /usr/bin/minicom <Telco_switch_name> Welcome to minicom 2.1 OPTIONS: History Buffer, F-key Macros, Search History Buffer, I18n Compiled on Jan 7 2007, 01:16:05. Press CTRL-A Z for help on special keys Press Enter Password: <Telco_switch_password> T5C-24GT> Switch> enable Password: <Telco_switch_enable_password> T5C-24GT#</pre> <p>If the enable command prompts for a password, the switch is not in a factory default configuration. This may be due to a previous configuration attempt. If this is the case, restore the factory default configuration by typing:</p> <pre>T5C-24GT# write erase wait ... T5C-24GT# reload no-save Proceed with reload? [y/n] : y Rebooting... [Additional output omitted]</pre> <p>The switch reboots to the factory default configuration. The following displays:</p> <pre>User Access Verification Password:</pre> |
| <p>7. <input type="checkbox"/></p> | <p>Management Server: Exit the switch console and minicom session</p> | <p>Type exit and press Enter to exit the console session.</p> <p>Exit the minicom session:</p> <ol style="list-style-type: none"> 1. Press Ctrl-A. 2. Press X. 3. Press Enter. |
| <p>8. <input type="checkbox"/></p> | <p>Management Server: Verify the switch configuration file exists</p> | <pre>\$ /bin/ls -l /usr/TKLC/plat/etc/vlan.conf /usr/TKLC/plat/etc/vlan.conf</pre> <p>If the file “vlan.conf” file does not exist, stop and contact Error! Bookmark not defined..</p> |
| <p>9. <input type="checkbox"/></p> | <p>Management Server: Verify the switch firmware binary exists</p> | <pre>\$ /bin/ls -l /var/TKLC/switchconfig/<T5CL3_24G_firmware_image_file></pre> <p>If the appropriate image does not exist, please check the T1200 Solutions Firmware Upgrade Pack (Tekelec part# 909-1618-001), or contact Error! Bookmark not defined..</p> |

Procedure 9. Replace a Failed Telco T5C-24GT

| Step | Procedure | Result |
|---------------------------------|--|--|
| 10. <input type="checkbox"/> | Management Server: Verify TFTP service is enabled | <pre>\$ /sbin/chkconfig --list tftp tftp off</pre> If the tftp service is set to off , turn on tftp by issuing the following command: <pre>\$ sudo /sbin/chkconfig tftp on</pre> Verify that it is now enabled: <pre>\$ /sbin/chkconfig --list tftp tftp on</pre> |
| 11. <input type="checkbox"/> | Management Server: Verify xinetd service is running | <pre>\$ sudo /sbin/service xinetd status</pre> If the output from the above command is: <pre>xinetd (pid xxxx) is running...</pre> Run the following command: <pre>\$ sudo /sbin/service xinetd restart Stopping xinetd: [OK] Starting xinetd: [OK]</pre> If the output from the above command is: <pre>xinetd is stopped</pre> Run the following command: <pre>\$ sudo /sbin/service xinetd start Starting xinetd: [OK]</pre> |
| 12. <input type="checkbox"/> | Management Server: Modify iptables to allow TFTP | Run iptablesAdm to modify iptables to allow the switch to pull configuration data from the server. <pre>\$ sudo iptablesAdm insert --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp --dport 69 -j ACCEPT" --location=1</pre> |
| 13. <input type="checkbox"/> | Management Server: Verify firewall is configured properly | <pre>\$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter Persist_Domain__Table__Chain__Match yes 10platnet filter INPUT -s <mgmt_network> -p udp --dport 69 -j ACCEPT</pre> |

Procedure 9. Replace a Failed Telco T5C-24GT

| Step | Procedure | Result |
|---------------------------------|---|--|
| 14. <input type="checkbox"/> | Management Server: Configure the switch | Run switchconfig to configure the switch. <pre>\$ sudo /usr/TKLC/plat/sbin/switchconfig -- swname=<Telco_switch_name> Successfully enabled on switch <Telco_switch_name>. Reloading switch <Telco_switch_name> with defaults, please standby... Switch <Telco_switch_name> successfully set to default configuration. Successfully started management VLAN on <Telco_switch_name>. Startup configuration created OK. Successfully uploaded startup config for <Telco_switch_name>. Removing config file <Telco_switch_name>.startup-config from /var/lib/tftpboot. Reloading switch <Telco_switch_name>, please standby... Reload of switch <Telco_switch_name> complete. Switch <Telco_switch_name> successfully configured.</pre> <p>Note: This step takes approximately 20 minutes to complete.</p> |
| 15. <input type="checkbox"/> | Management Server: Stop the xinetd service | Stop the xinetd service once the switch has been upgraded and configured: <pre>\$ sudo /sbin/service xinetd stop Stopping xinetd:</pre> |
| 16. <input type="checkbox"/> | Management Server: Disable TFTP services | Disable the tftp service by running the following command: <pre>\$ sudo /sbin/chkconfig tftp off</pre> |
| 17. <input type="checkbox"/> | Telco T5CL3_24G: Connect uplink cables | Connect the uplink cables from the new Telco switch to the customer network. |
| 18. <input type="checkbox"/> | Management Server: Test switches | To ensure traffic is flowing through both Telco switches properly after a RMA procedure, start up a ping on each T1200 server: <pre>\$ /bin/ping <Remote_customer_target_ip></pre> <p>Notes</p> <ul style="list-style-type: none"> • If the management server is a SOAM, use the IP address of the NOAM VIP for <Remote_customer_target_ip>. • If the management server is an NOAM, use the address of the SOAM VIP for <Remote_customer_target_ip>. <p>With these pings running on each server, perform the following steps:</p> <ol style="list-style-type: none"> 1. On the Management Server connected to the replacement Telco switch, force it to use eth01 by running the following command: <pre>\$ sudo /sbin/ifenslave -c bond1 eth01</pre> 2. On the mated Management server connected to the mated Telco switch, force it to use eth02 by running the following command: |

Procedure 9. Replace a Failed Telco T5C-24GT

| Step | Procedure | Result |
|------|-----------|--|
| | | <pre data-bbox="548 302 1081 327">\$ sudo /sbin/ifenslave -c bond1 eth02</pre> <p data-bbox="548 338 1393 401">If either server is not pinging correctly or has stopped responding at this point, please contact Error! Bookmark not defined..</p> <ol data-bbox="500 415 1419 982" style="list-style-type: none"> <li data-bbox="500 415 1419 447">3. On the new/replacement Telco switch, unplug the customer uplink cables. <li data-bbox="500 464 1419 527">4. Verify the pings from each server are still reaching <Remote_customer_target_ip>. <p data-bbox="548 537 1354 600">There may be a brief pause after unplugging the uplink cables as the mated switch takes over the VRRP interfaces (less than 5 seconds).</p> <ul data-bbox="548 615 1414 789" style="list-style-type: none"> <li data-bbox="548 615 1414 678">• If the pings are no longer reaching <Remote_customer_target_ip> on both servers, stop and contact Error! Bookmark not defined.. <li data-bbox="548 695 1414 789">• If the pings continue, this verifies the mated switch is performing as expected by sending traffic to the customer network, and traffic is flowing to it over the ISL from the replacement Telco switch. <ol data-bbox="500 804 1382 982" style="list-style-type: none"> <li data-bbox="500 804 1382 867">5. Replace the uplink cables to the customer network on the replacement Telco switch. <li data-bbox="500 884 1382 915">6. On the mated Telco switch, unplug the customer uplink cables. <li data-bbox="500 932 1382 982">7. Verify the pings from each server are still reaching <Remote_customer_target_ip>. <p data-bbox="548 999 1390 1094">Again, there may be a brief pause after unplugging the uplink cables as the replaced Telco switch takes over the VRRP interfaces (less than 5 seconds).</p> <ul data-bbox="548 1108 1414 1272" style="list-style-type: none"> <li data-bbox="548 1108 1414 1171">• If the pings are no longer reaching <Remote_customer_target_ip> on both servers, stop and contact Error! Bookmark not defined.. <li data-bbox="548 1188 1414 1272">• If the pings continue, this verifies traffic is flowing over the replacement Telco switch to the customer network and over the ISL and that both switches are functioning as expected. <ol data-bbox="500 1287 1382 1350" style="list-style-type: none"> <li data-bbox="500 1287 1382 1350">8. Replace the uplink cables to the customer network on the replacement Telco switch. |

Procedure 9. Replace a Failed Telco T5C-24GT

| Step | Procedure | Result |
|---------------------------------|--|---|
| 19. <input type="checkbox"/> | Management Server: Disable TFTP | <p>Execute the commands that disable tftp transfer.</p> <pre>\$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd stopXinetdService service tftp force yes Login on Remote: platcfg Password of platcfg: <platcfg_password> 1</pre> <p>Ensure the tftp service is not running by executing the following command. A zero is expected.</p> <pre>\$ sudo /usr/TKLC/plat/bin/tpdProvd --client --noxml --ns=Xinetd getXinetdService service tftp Login on Remote: platcfg Password of platcfg: <platcfg_password> 0</pre> <p>If a 1 is returned, repeat this step until getXinetdService returns a zero.</p> |
| 20. <input type="checkbox"/> | Management Server: Remove the iptables rule to allow TFTP | <pre>\$ sudo iptablesAdm delete --type=rule --protocol=ipv4 --domain=10platnet --table=filter --chain=INPUT --persist=yes --match="-s <mgmt_network> -p udp --dport 69 -j ACCEPT"</pre> |
| 21. <input type="checkbox"/> | Management Server: Verify the firewall is configured properly | <pre>\$ sudo iptablesAdm show --type=rule --protocol=ipv4 --chain=INPUT --domain=10platnet --table=filter Persist__Domain__Table__Chain__Match</pre> |

3.3 C-Class Enclosure Switch — netConfig Procedures

3.3.1 Configure Cisco 3020 Switch (netConfig)

This procedure configures 3020 switches from the PMAC server using templates included with an application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- If the aggregation switches are supported by Oracle, the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.

- No IPM switches activity can occur during the execution of this procedure.

Note: The Cisco 3020 is not compatible with the IPv6 management configuration.

Needed Material

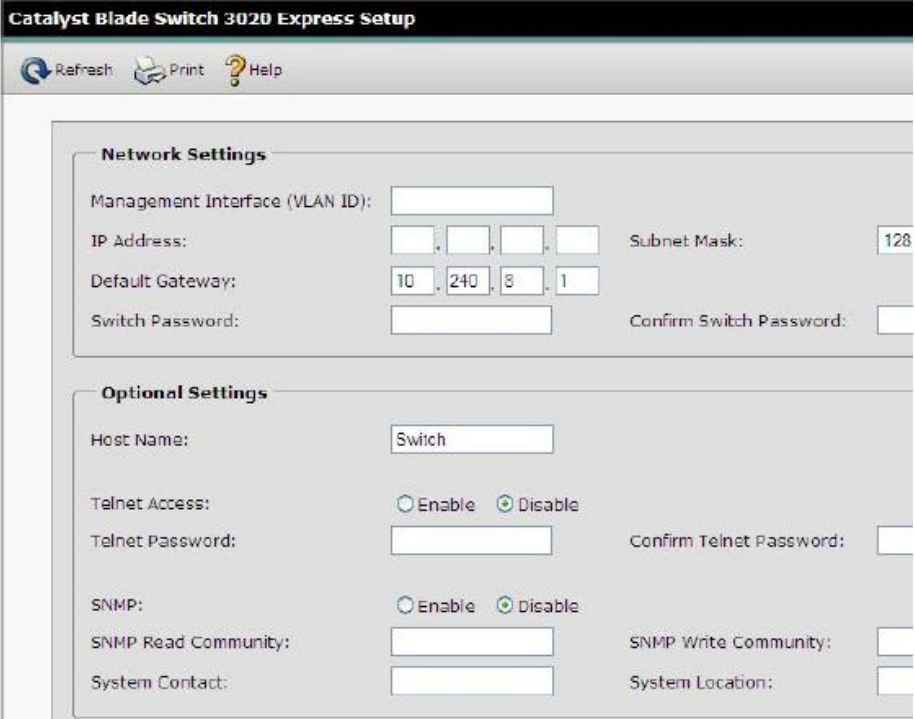
- HP MISC Firmware ISO image
- Refer to the [4] Oracle Firmware Upgrade Pack Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

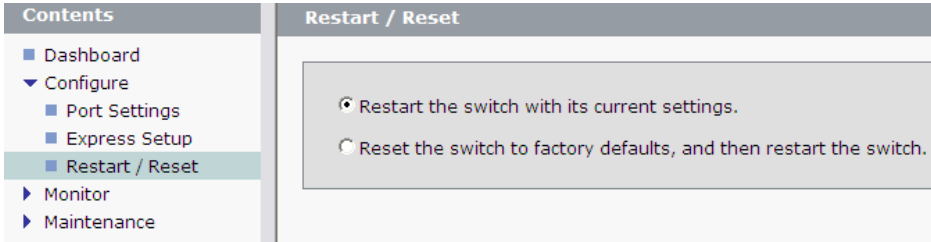
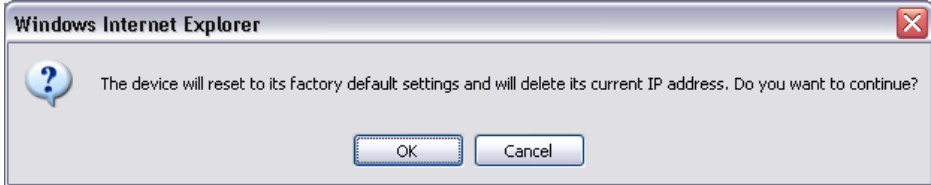
Procedure 10. Configure Cisco 3020 Switch (netConfig)

| Step | Procedure | Result |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Virtual PMAC: Prepare for switch configuration | Login as admusr to the PMAC, then run: <pre>\$ /bin/ping -w3 <mgmtVLAN_gateway_address></pre> |
| 2. <input type="checkbox"/> | Virtual PMAC: Verify network connectivity | For each 3020 switch, verify network reachability. <pre>\$ /bin/ping -w3 <enclosure_switch_IP></pre> |
| 3. <input type="checkbox"/> | Virtual PMAC: Modify PMAC feature to allow TFTP | Enable the DEVICE.NETWORK.NETBOOT feature with the management role to allow tftp traffic: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm editFeature -- featureName=DEVICE.NETWORK.NETBOOT --enable=1</pre> <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures</pre> Note: This may take up to 60 seconds to complete. |
| 4. <input type="checkbox"/> | Virtual PMAC: Verify template xml files exist | Verify the initialization xml and configuration xml template files are present on the system and are the correct version for the system. Note: The XML files prepared in advance with the NAPD can be used as alternatives. <pre>\$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_init.xml</pre> <pre>\$ /bin/more /usr/TKLC/smac/etc/switch/xml/3020_configure.xml</pre> If either file does not exist, copy the files from the application media into the directory. If 3020_init.xml file exists, page through the contents to verify it is devoid of any site-specific configuration information other than the device name. If the template file is appropriate, then continue to step 6. If 3020_configure.xml file exists, page through the contents to verify it is the appropriate file for this site and edited for this site. All network information is necessary for this activity. If the template file is appropriate, then continue to step 6. |

Procedure 10. Configure Cisco 3020 Switch (netConfig)

| Step | Procedure | Result |
|--|--|---|
| <p>5. <input type="checkbox"/></p> | <p>Virtual PMAC: Modify 3020 xml files for information needed to configure the switch</p> | <p>Update 3020_init.xml file: <code>\$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_init.xml</code></p> <p>Update 3020_configure.xml file: <code>sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/3020_config.xml</code></p> <p>Note: Modify values notated with a preceding dollar sign. So a value with <code>\$some_variable_name</code> needs to be modified. Remove the dollar sign and the less than, greater than sign.</p> <p>When editing is complete, save the file and quit.</p> |
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC/OA GUI: Reset switch to factory defaults</p> | <ol style="list-style-type: none"> If the switch has been previously configured using netConfig or previous attempts at initialization have failed, use netConfig to reset the switch to factory defaults by executing the following command: <code>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> setFactoryDefault</code> If the command fails, use Internet Explorer to navigate to <code><enclosure_switch_ip_address></code>. If you are asked for a username and password, leave the username blank and use the appropriate password provided by the application documentation. Click OK. If you are prompted with the Express Setup screen, click Refresh.  <ol style="list-style-type: none"> If you are prompted with Do you want a secured session with the switch?, click No. <p>A new Catalyst Blade Switch 3020 Device Manager displays.</p> |

Procedure 10. Configure Cisco 3020 Switch (netConfig)

| Step | Procedure | Result |
|------------------------------------|--|--|
| | | <p>6. Navigate to Configure -> Restart/Reset.</p>  <p>7. Select the Reset the switch to factory defaults, and then restart the switch option.</p> <p>8. Click Submit.</p> <p>9. Click OK to continue with the reset.</p>  <p>Note: Do not wait for the switch to finish reloading before proceeding to the next step.</p> |
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Remove the old ssh key and initialize the switch</p> | <p>Remove the old ssh key:</p> <pre>\$ sudo /usr/bin/ssh-keygen -R <enclosure_switch_ip></pre> <p>The following command must be entered at least 60 seconds and at most 5 minutes after the previous step is completed.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/3020_init.xml Processing file: /usr/TKLC/smac/etc/switch/xml/3020_init.xml Waiting to load the configuration file... loaded. Attempting to login to device... Configuring....</pre> <p>Note: This step takes about 10-15 minutes to complete. It is imperative that you wait until returned to the command prompt. DO NOT PROCEED UNTIL RETURNED TO THE COMMAND PROMPT.</p> <p>Check the output of this command for any errors. A successful completion of netConfig returns the user to the prompt. Due to strict host checking and the narrow window of time in which to perform the command, this command is prone to user error. Most issues are corrected by returning to the previous step and continuing. If this step has failed for a second time, stop the procedure and contact Error! Bookmark not defined.</p> |

Procedure 10. Configure Cisco 3020 Switch (netConfig)

| Step | Procedure | Result |
|---------------------------------|---|--|
| 8. <input type="checkbox"/> | Virtual PMAC: Reboot the switch using netConfig | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> reboot save=no</pre> <p>Wait 2-3 minutes for the switch to reboot. Verify it has completed rebooting and is reachable by pinging it.</p> <pre>\$ /bin/ping <enclosure_switch_IP> From 10.240.8.48 icmp_seq=106 Destination Host Unreachable From 10.240.8.48 icmp_seq=107 Destination Host Unreachable From 10.240.8.48 icmp_seq=108 Destination Host Unreachable 64 bytes from 10.240.8.13: icmp_seq=115 ttl=255 time=1.13 ms 64 bytes from 10.240.8.13: icmp_seq=116 ttl=255 time=1.20 ms 64 bytes from 10.240.8.13: icmp_seq=117 ttl=255 time=1.17 ms</pre> |
| 9. <input type="checkbox"/> | Virtual PMAC: Validate XML file | <p>This script validates the XML file to a limited extent. It verifies:</p> <ul style="list-style-type: none"> • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values <p>To validate the XML file:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -file=3020_configure.xml -testRun > dev/null</pre> <p>If nothing is returned then the XML file is valid to the extent defined above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.</p> |
| 10. <input type="checkbox"/> | Virtual PMAC: Configure the switches | <p>Configure both switches by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/3020_configure.xml Processing file: /usr/TKLC/smac/etc/switch/xml/3020_configure.xml</pre> <p>Note: This may take up to 2-3 minutes to complete.</p> <p>Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns the user to the prompt.</p> |

Procedure 10. Configure Cisco 3020 Switch (netConfig)

| Step | Procedure | Result |
|---------------------------------|---|--|
| 11. <input type="checkbox"/> | Virtual PMAC: Verify switch configuration | To verify the configuration was completed successfully, execute the following command and review the configuration: <pre># sudo /usr/TKLC/plat/bin/netConfig showConfiguration -- device=<switch_name> Configuration: = (Building configuration... Current configuration : 3171 bytes ! ! Last configuration change at 23:54:24 UTC Fri Apr 2 1993 by plat ! version 12.2 <output removed to save space > monitor session 1 source interface Gi0/2 rx monitor session 1 destination interface Gi0/1 encapsulation replicate end)</pre> Return to step 4. and repeat for each 3020 switch. |
| 12. <input type="checkbox"/> | Virtual PMAC: Modify PMAC feature to disable TFTP | Disable the DEVICE.NETWORK.NETBOOT feature: <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm editFeature -- featureName=DEVICE.NETWORK.NETBOOT --enable=0 \$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures</pre> Note: This may take up to 60 seconds to complete. |
| 13. <input type="checkbox"/> | Virtual PMAC: Repeat | Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig) for each switch configured in this procedure. |
| 14. <input type="checkbox"/> | Virtual PMAC: Clean up FW file | Remove the FW file from the tftp directory. <pre>\$ sudo /bin/rm -f /var/TKLC/smac/image/<FW_image></pre> |

3.3.2 Replace a Failed 3020 Switch (netConfig)

This procedure configures a replacement 3020 switch.

Prerequisite: User has determined which switch has failed.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate value from [2] HP Solutions Firmware Upgrade Pack.

| Variable | Cisco 4948 | Cisco 4948E | Cisco 4948E-F |
|------------------|------------|-------------|---------------|
| <IOS_image_file> | | | |

Needed Material: HP MISC firmware ISO image

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 11. Replace a Failed 3020 Switch

| Step | Procedure | Result |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Cabinet: Replace switch | Remove failed switch and replace with new switch of same model. |
| 2. <input type="checkbox"/> | Cabinet: Attach cable to new switch | Connect all network and console cables to the new switch. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch. Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink. |
| 3. <input type="checkbox"/> | Virtual PMAC: Move firmware image | Firmware version must be identical between mating switches, to check the firmware on the mate switch use the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=<switch_hostname> getFirmware</pre> Move the appropriate FW image from the switch backup directory to the TFTP directory by performing the following command: For a PMAC System: <pre>\$ sudo /bin/mv -i <switch_backup_directory/<FW_image> /var/TKLC/smac/image/</pre> For a non-PMAC System: <pre>\$ sudo /bin/mv -i <switch_backup_directory/<FW_image> /var/lib/tftpboot/</pre> Note: If the file does not exist on the server, copy it from the firmware media. |
| 4. <input type="checkbox"/> | Virtual PMAC: Apply configuration | Perform 3.3.1 Configure Cisco 3020 Switch (netConfig), steps 3. through 9. and 12. , replacing the values for the switch being replaced. |
| 5. <input type="checkbox"/> | Virtual PMAC: Restore the switch to the latest known good configuration | Navigate to the <switch_backup_user> home directory. <pre>\$ cd ~<switch_backup_user></pre> Verify your location on the server <pre>\$ /bin/pwd</pre> <pre>/home/<switch_backup_user></pre> |
| 6. <input type="checkbox"/> | Virtual PMAC: Copy switch backup file | Copy the switch backup files to the home directory of the <switch_backup_user> by performing the following command: <pre>\$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup* /home/<switch_backup_user>/</pre> Get a list of the file copied over. Note: 'switch1A' is shown as an example. <pre>\$ /bin/ls -l</pre> <pre>switch1A-backup</pre> <pre>switch1A-backup.info</pre> <pre>switch1A-backup.vlan</pre> |

Procedure 11. Replace a Failed 3020 Switch

| Step | Procedure | Result |
|---------------------------------|--|---|
| 7. <input type="checkbox"/> | Virtual PMAC: Verify switch is initialized | Verify switch is initialized correctly and connectivity to the switch by verifying the hostname. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> getHostname Hostname: switch1A</pre> Note: The value beside Hostname should be the same as the <switch_name> variable. |
| 8. <input type="checkbox"/> | Virtual PMAC: Restore | <pre>\$ cd ~<switch_backup_user> \$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>- backup* \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> restoreConfiguration service=ssh_service filename=<switch_hostname>-backup</pre> Note: If the command failed with error message same as or similar to Error saving to service , and the TPD version is 7.6.0.0.0_88.50.0 or later, refer to Appendix T . |
| 9. <input type="checkbox"/> | Virtual PMAC: Verify connectivity | Perform 3.3.1 Configure Cisco 3020 Switch (netConfig), step 10. |
| 10. <input type="checkbox"/> | Virtual PMAC: Clean up FW | Remove the FW images from the users' home directory and TFTP directory with the following command: <pre>\$ sudo rm ~admusr/<fw_filename> \$ sudo rm /var/TKLC/snac/image/<fw_filename></pre> |

3.3.3 Configure HP 6120XG Switch (netConfig)

This procedure configures the HP 6120XG switches from the PMAC server and the command line interface using templates included with an application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- If the aggregation switches are supported by Oracle, the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.
- Must be able to issue commands on the switch command line interface

Needed Material

- HP MISC Firmware ISO image

- Refer to the [4] Oracle Firmware Upgrade Pack Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

Note: The HP 6120XG switch requires router advertisements for learning the IPv6 default route. No manual IPv6 default route can be configured on this switch.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 12. Configure HP 6120XG Switch

| Step | Procedure | Result |
|-----------------|--|---|
| <p>1. □</p> | <p>Virtual PMAC: Prepare for switch configuration</p> | <p>If aggregation switches are supported by Oracle, log into the management server as admusr to the PMAC, then run:</p> <pre data-bbox="548 646 1166 741"> \$ /bin/ping -w3 <switch1A_mgmtVLAN_address> \$ /bin/ping -w3 <switch1B_mgmtVLAN_address> \$ /bin/ping -w3 <switch_mgmtVLAN_VIP> </pre> <p>If aggregation switches are provided by customer, log into the management server as admusr to the PMAC, then run:</p> <pre data-bbox="548 825 1166 846"> \$ /bin/ping -w3 <mgmtVLAN_gateway_address> </pre> |
| <p>2. □</p> | <p>Virtual PMAC: Verify network connectivity</p> | <p>For each 6120XG switch, verify network reachability.</p> <pre data-bbox="548 909 1084 930"> \$ /bin/ping -w3 <enclosure_switch_IP> </pre> |

Procedure 12. Configure HP 6120XG Switch

| Step | Procedure | Result |
|--|---|--|
| <p>3. <input type="checkbox"/></p> | <p>Virtual PMAC: Reset switch to factory defaults</p> | <p>If the 6120XG switch has been configured before this procedure, clear the configuration using the following command:</p> <pre>\$ /usr/bin/ssh <username>@<enclosure_switch_IP> Switch# config Switch(config)# no password all Password protection for all will be deleted, continue [y/n]? y Switch(config)# end Switch# erase startup-config Configuration will be deleted and device rebooted, continue [y/n]? y (switch will automatically reboot, reboot takes about 120-180 seconds)</pre> <p>Note: You may need to press [ENTER] twice. You may also need to use previously configured credentials.</p> <p>If the command fails, login using telnet and reset the switch to manufacturing defaults.</p> <pre>\$ /usr/bin/telnet <enclosure_switch_IP> Switch# config Switch(config)# no password all (answer yes to question) Password protection for all will be deleted, continue [y/n]? y Switch(config)# end Switch# erase startup-config (switch will automatically reboot, reboot takes about 120-180 seconds)</pre> <p>Note: The console connection to the switch must be closed, or the initialization fails.</p> |
| <p>4. <input type="checkbox"/></p> | <p>Virtual PMAC: Copy switch configuration template from media to TFTP directory</p> | <pre>\$ sudo /bin/cp -i /<path to media>/6120XG_init.xml /usr/TKLC/smac/etc/switch/xml \$ sudo /bin/cp -i /<path to media>/6120XG_[single,LAG]Uplink_configure.xml /usr/TKLC/smac/etc/switch/xml \$ sudo /bin/cp -i /usr/TKLC/plat/etc/TKLNetwork-config-templates/templates/utility/addQOS_trafficTemplate_6120XG.xml /usr/TKLC/smac/etc/switch/xml</pre> <p>where [single, LAG] are variables for either of these files:</p> <ul style="list-style-type: none"> • 6120XG_SingleUplink_configure.xml is for one uplink per enclosure switch topology • 6120XG_LAGUplink_configure.xml is for LAG uplink topology |

Procedure 12. Configure HP 6120XG Switch

| Step | Procedure | Result |
|--|---|---|
| <p>5. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify switch configuration</p> | <p>Verify the switch initialization and configuration template files are in the correct directory.</p> <pre>\$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/ -rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6120XG_init.xml -rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml -rw-r--r-- 1 root root 702 Sep 10 10:33 addQOS_trafficTemplate_6120XG.xml</pre> |
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC: Edit switch configuration file template for site-specific information</p> | <p>Modify values notated with a preceding dollar sign (for example, addresses and VLAN IDs). So a value with <code>\$some_variable_name</code> needs to be modified. Remove the dollar sign and the less than, greater than sign.</p> <p>Note: Files created in this step can be prepared ahead of time using NAPD.</p> <pre>\$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6120XG_init.xml \$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml \$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml</pre> |
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Apply <code>include-credentials</code> command to the switch</p> | <p>Log into the switch using ssh.</p> <pre>\$ /usr/bin/ssh <username>@<enclosure_switch_IP> Switch# config Switch(config)# include-credentials If prompted, answer yes to both questions. Log out of the switch. Switch(config)# logout Do you want to log out [y/n]? y Do you want to save current configuration [y/n/^C]? y</pre> |
| <p>8. <input type="checkbox"/></p> | <p>Virtual PMAC: Initialize the switch</p> | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/6120XG_init.xml Processing file: /usr/TKLC/smac/etc/switch/xml/3020_init.xml Waiting to load the configuration file... loaded. Attempting to login to device... Configuring....</pre> <p>Note: This step takes 5-10 minutes to complete.</p> <p>The user is returned to the PMAC command prompt. If netConfig fails to complete successfully, contact Error! Bookmark not defined.</p> |

Procedure 12. Configure HP 6120XG Switch

| Step | Procedure | Result |
|---------------------------------|---|--|
| 9. <input type="checkbox"/> | Virtual PMAC: Validate XML file | <p>This script validates the XML file to a limited extent. It verifies:</p> <ul style="list-style-type: none"> • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values <p>To validate the XML file:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig - file=6120XG_[single,LAG]Uplink_configure.xml -testRun > dev/null</pre> <p>If nothing is returned then the XML file is valid to the extent defined above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.</p> |
| 10. <input type="checkbox"/> | Virtual PMAC: Configure the switches | <p>Configure both switches by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/3020_configure.xml</pre> <p>Processing file: /usr/TKLC/smac/etc/switch/xml/6120XG_[single,LAG]Uplink_configure.xml</p> <p>Note: This may take up to 2-3 minutes to complete.</p> <p>Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns the user to the prompt.</p> |
| 11. <input type="checkbox"/> | Virtual PMAC: Apply QoS settings | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/addQOS_trafficTemplate_6120XG.xml</pre> <p>Note: The switch reboots after this command. This step takes 2-5 minutes.</p> |
| 12. <input type="checkbox"/> | Virtual PMAC: Verify proper configuration of switches | <p>Verify network reachability and configuration.</p> <pre>\$ /bin/ping -w3 <enclose_switch_IP> \$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP> <switch_platform_username>@<enclosure_switch_IP>'s password: <switch_platform_password> Switch# show run</pre> <p>Inspect the output and ensure it is configured per site requirements.</p> |
| 13. <input type="checkbox"/> | Virtual PMAC: Repeat | Repeat steps 3. through 12. for each HP 6120XG. |
| 14. <input type="checkbox"/> | Back up HP for each switch | Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure. |

Procedure 12. Configure HP 6120XG Switch

| Step | Procedure | Result |
|---------------------------------|-------------------------------------|--|
| 15. <input type="checkbox"/> | Virtual PMAC: Clean up FW | Remove the FW image from the users' home directory and TFTP directory with the following command: <code>\$ sudo /bin/rm -f ~<switch_backup_user>/<fw_filename></code> |

3.3.4 Configure HP 6125G Switch (netConfig)

This procedure configures the HP 6125G switches from the PMAC server and the command line interface using templates included with the application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- Must be able to issue commands on the switch command line interface
- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.

Needed Material

- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 13. Configure HP 6125G Switch

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Virtual PMAC: Prepare for switch configuration | If the aggregation switches are supported by Oracle, login as admusr to the PMAC, then run: <code>\$ /bin/ping -w3 <switch1A_mgmtVLAN_address></code> <code>\$ /bin/ping -w3 <switch1B_mgmtVLAN_address></code> <code>\$ /bin/ping -w3 <switch_mgmtVLAN_VIP></code> If the aggregation switches are provided by the customer, login as admusr to the PMAC, then run: <code>\$ /bin/ping -w3 <mgmtVLAN_gateway_address></code> |
| 2. <input type="checkbox"/> | Virtual PMAC: Verify network connectivity | For each OA, verify network reachability. <code>\$ /bin/ping -w3 <OA1_IP></code> <code>\$ /bin/ping -w3 <OA2_IP></code> |
| 3. <input type="checkbox"/> | Virtual PMAC: Determine which OA is | Login to OA1 to determine if it is active: <code>\$ /usr/bin/ssh root@<OA1_IP></code> The OA is active if you see the following: |

Procedure 13. Configure HP 6125G Switch

| Step | Procedure | Result |
|------|--|---|
| | currently active | <pre>Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: If you see the following, it is standby: Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 1 OA Role: Standby root@10.240.8.5's password: Press Ctrl + C to close the SSH session. If OA1 has a role of standby, verify that OA2 is the active by logging into it: \$ /usr/bin/ssh root<OA2_IP> Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: In the following steps, OA refers to the active OA and <active_OA_IP> refers to the IP address of the active OA. Note: If no OA reports active, STOP and contact Error! Bookmark not defined. Exit the SSH session.</pre> |
| 4. | Virtual PMAC: Restore switch | If the 6125G switch has been configured before this procedure, clear the configuration using the following command: |

Procedure 13. Configure HP 6125G Switch

| Step | Procedure | Result |
|----------|----------------------------|--|
| <p>□</p> | <p>to factory defaults</p> | <pre> \$/usr/bin/ssh root@<active_OA_IP> Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: <OA_password> > connect interconnect <switch_IOBAY_#> Press [Enter] to display the switch console: Note: You may need to press ENTER twice. You may also need to use previously configured credentials. <switch>reset saved-configuration The saved configuration file will be erased. Are you sure? [Y/N]:y Configuration file in flash is being cleared. Please wait ... MainBoard: Configuration file is cleared. <switch>reboot Start to check configuration with next startup configuration file, please wait.....DONE! This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]:n This command will reboot the device. Continue? [Y/N]: y The switch automatically reboots. This takes 120-180 seconds. The switch reboot is complete when you see the following text: [...Output omitted...] User interface aux0 is available. Press ENTER to get started. When the reboot is complete, disconnect from the console by pressing Ctrl + Shift + -, then d. Note: If connecting to the virtual PMAC through the management server iLO then Appendix E.1 Access a Server Console Remotely applies. Disconnect from the console by pressing Ctrl +v. Exit from the OA terminal: >exit Note: The console connection to the switch must be closed or the initialization fails. </pre> |

Procedure 13. Configure HP 6125G Switch

| Step | Procedure | Result |
|---------------------------------|---|--|
| 5. <input type="checkbox"/> | Virtual PMAC: Copy switch configuration template from media to TFTP directory | <pre>\$ sudo /bin/cp -i /<path to media>/6125G_init.xml /usr/TKLC/smac/etc/switch/xml \$ sudo /bin/cp -i /<path to media>/6125G_configure.xml /usr/TKLC/smac/etc/switch/xml</pre> |
| 6. <input type="checkbox"/> | Virtual PMAC: Verify switch configuration | <p>Verify the switch initialization and configuration template files are in the TFTP directory.</p> <pre>\$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/ -rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6125G_init.xml -rw-r--r-- 1 root root 1955 Feb 16 11:36 /usr/TKLC/smac/etc/switch/xml/6125G_configure.xml</pre> |
| 7. <input type="checkbox"/> | Virtual PMAC: Edit switch configuration file template for site-specific information | <p>Modify values notated with a preceding dollar sign (for example, addresses and VLAN IDs). So a value with <code>\$some_variable_name</code> needs to be modified. Remove the dollar sign and the less than, greater than sign.</p> <p>Note: Files created in this step can be prepared ahead of time using NAPD.</p> <pre>\$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125G_init.xml \$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125G_configure.xml</pre> |
| 8. <input type="checkbox"/> | Virtual PMAC: Initialize the switch | <p>Note: The console connection to the switch must be closed or the initialization fails.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/6125G_init.xml</pre> <p>Note: This step takes 5-10 minutes to complete.</p> |
| 9. <input type="checkbox"/> | Virtual PMAC: Verify switch initialized | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig getHostname -- device=<switch_hostname> Hostname: <switch_hostname></pre> <p>Note: This step takes 2-3 minutes to complete.</p> <p>The user is returned to the PMAC command prompt. If netConfig fails to complete successfully, contact Error! Bookmark not defined.</p> |
| 10. <input type="checkbox"/> | Virtual PMAC | Execute Appendix J Downgrade Firmware on a 6125G Switch to verify the existing firmware version and downgrade if required |

Procedure 13. Configure HP 6125G Switch

| Step | Procedure | Result |
|---------------------------------|--|--|
| 11. <input type="checkbox"/> | Virtual PMAC: Validate XML file | <p>This script validates the XML file to a limited extent. It verifies:</p> <ul style="list-style-type: none"> • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values <p>To validate the XML file:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -file=6125G_configure.xml -testRun > dev/null</pre> <p>If nothing is returned then the XML file is valid to the extent defined above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.</p> |
| 12. <input type="checkbox"/> | Virtual PMAC: Configure the switch | <p>Configure the switch by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/6125G_configure.xml Processing file: /usr/TKLC/smac/etc/switch/xml/6125G_configure.xml</pre> <p>Note: This may take up to 2-3 minutes to complete.</p> <p>Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns the user to the prompt.</p> |
| 13. <input type="checkbox"/> | Virtual PMAC: Add IPv6 default route (IPv6 network only) | <p>For IPv6 management networks, the enclosure switch requires an IPv6 default route to be configured. Apply the following command using netConfig:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addRoute network=::/0 nexthop=<mgmtVLAN_gateway_address></pre> |
| 14. <input type="checkbox"/> | Virtual PMAC: Verify proper configuration of switch | <p>Once the HP 6125G has finished booting from the previous step, verify network reachability and configuration.</p> <pre>\$ /bin/ping -w3 <enclosure_switch_IP> PING 10.240.8.10 (10.240.8.10) 56(84) bytes of data.64 bytes from 10.240.8.10: icmp_seq=1 ttl=255 time=0.637 ms64 bytes from 10.240.8.10: icmp_seq=2 ttl=255 time=0.661 ms64 bytes from 10.240.8.10: icmp_seq=3 ttl=255 time=0.732 m \$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP> <switch_platform_username>@<enclosure_switch_IP>'s password: <switch_platform_password> Switch_hostname> display current-configuration</pre> <p>Inspect the output and ensure it is configured as per site requirements.</p> |
| 15. <input type="checkbox"/> | Virtual PMAC: Repeat | Repeat steps 4. through 14. for each HP 6125G switch. |
| 16. <input type="checkbox"/> | Virtual PMAC | Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure. |

Procedure 13. Configure HP 6125G Switch

| Step | Procedure | Result |
|---------------------------------|--|---|
| 17. <input type="checkbox"/> | Virtual PMAC: Clean up FW file | Remove the FW file from the tftp directory. <pre>\$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image></pre> |

3.3.5 Configure HP 6125XLG Switch (netConfig)

This procedure configures the HP 6125XLG switches from the PMAC server and the command line interface using templates included with the application.

Prerequisites:

- PMAC must be installed
- 3.1 Configure netConfig Repository
- 7.1 Configure Initial OA IP
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- Must be able to issue commands on the switch command line interface
- If the aggregation switches are supported by Oracle, the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.

Needed Material

- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 14. Configure HP 6125XLG Switch

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Virtual PMAC: Prepare for switch configuration | If the aggregation switches are supported by Oracle, login as admusr to the PMAC, then run: <pre>\$ /bin/ping -w3 <switch1A_mgmtVLAN_address> \$ /bin/ping -w3 <switch1B_mgmtVLAN_address> \$ /bin/ping -w3 <switch_mgmtVLAN_VIP></pre> If the aggregation switches are provided by the customer, login as admusr to the PMAC, then run: <pre>\$ /bin/ping -w3 <mgmtVLAN_gateway_address></pre> |
| 2. <input type="checkbox"/> | Virtual PMAC: Verify network connectivity | For each OA, verify network reachability. <pre>\$ /bin/ping -w3 <OA1_IP> \$ /bin/ping -w3 <OA2_IP></pre> |
| 3. <input type="checkbox"/> | Virtual PMAC: Determine which OA is | Login to OA1 to determine if it is active: <pre>\$ /usr/bin/ssh root@<OA1_IP></pre> The OA is active if you see the following: |

Procedure 14. Configure HP 6125XLG Switch

| Step | Procedure | Result |
|--------------------------------|--|--|
| | currently active | <pre>Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: If you see the following, it is standby: Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 1 OA Role: Standby root@10.240.8.5's password: Press Ctrl + C to close the SSH session. If OA1 has a role of standby, verify that OA2 is the active by logging into it: \$ /usr/bin/ssh root@<OA2_IP> Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: In the following steps, OA refers to the active OA and <active_OA_IP> refers to the IP address of the active OA. Note: If no OA reports active, STOP and contact Error! Bookmark not defined.. Exit the SSH session.</pre> |
| 4. <input type="checkbox"/> | Virtual PMAC: Restore switch to factory defaults | <pre>If the 6125XLG switch has been configured before this procedure, clear the configuration using the following command: \$/usr/bin/ssh root@<active_OA_IP> Using username "root". ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in</pre> |

Procedure 14. Configure HP 6125XLG Switch

| Step | Procedure | Result |
|------------------------------------|---|--|
| | | <pre> criminal or civil prosecution under applicable law. ----- Firmware Version: 3.70 Built: 10/01/2012 @ 17:53 OA Bay Number: 2 OA Role: Active root@10.240.8.6's password: <OA_password> > connect interconnect <switch_IOBAY_#> Press [Enter] to display the switch console: Note: You may need to press ENTER twice. You may also need to use previously configured credentials. <switch>reset saved-configuration The saved configuration file will be erased. Are you sure? [Y/N]:y Configuration file in flash is being cleared. Please wait ... MainBoard: Configuration file is cleared. <switch>reboot Start to check configuration with next startup configuration file, please wait.....DONE! This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]:n This command will reboot the device. Continue? [Y/N]: y The switch automatically reboots. This takes 120-180 seconds. The switch reboot is complete when you see the following text: [...Output omitted...] User interface aux0 is available. Press ENTER to get started. When the reboot is complete, disconnect from the console by pressing Ctrl + Shift + -, then d. Note: If connecting to the virtual PMAC through the management server iLO then Appendix E.1 Access a Server Console Remotely applies. Disconnect from the console by pressing Ctrl +v. Exit from the OA terminal: >exit Note: The console connection to the switch must be closed or the initialization fails. </pre> |
| <p>5. <input type="checkbox"/></p> | <p>Virtual PMAC: Copy switch configuration template from media to TFTP directory</p> | <pre> \$ sudo /bin/cp -i /<path to media>/6125XLG_init.xml /usr/TKLC/smac/etc/switch/xml \$ sudo /bin/cp -i /<path to media>/6125XLG_configure.xml /usr/TKLC/smac/etc/switch/xml </pre> |

Procedure 14. Configure HP 6125XLG Switch

| Step | Procedure | Result |
|---|---|--|
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify switch configuration</p> | <p>Verify the switch initialization and configuration template files are in the TFTP directory.</p> <pre>\$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/xml/ 131195 -rw----- 1 root root 248 May 5 11:01 6125XLG_IOBAY3_template_init.xml 131187 -rw----- 1 root root 248 May 5 10:54 6125XLG_IOBAY5_template_init.xml 131190 -rw----- 1 root root 6194 Mar 24 15:04 6125XLG_IOBAY8-config.xml 131189 -rw----- 1 root root 248 Mar 25 09:43 6125XLG_IOBAY8_template_init.xml</pre> |
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Edit switch configuration file template for site-specific information</p> | <p>Modify values notated with a preceding dollar sign (for example, addresses and VLAN IDs). So a value with <code>\$some_variable_name</code> needs to be modified. Remove the dollar sign and the less than, greater than sign.</p> <p>Note: Files created in this step can be prepared ahead of time using NAPD.</p> <pre>\$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125XLG_init.xml \$ sudo /bin/vi /usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml</pre> |
| <p>8. <input type="checkbox"/></p> | <p>Virtual PMAC: Initialize the switch</p> | <p>Note: The console connection to the switch must be closed or the initialization fails.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/6125XLG_init.xml</pre> <p>Note: This step takes 5-10 minutes to complete.</p> |
| <p>9. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify switch initialized</p> | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig getHostname -- device=<switch_hostname> Hostname: <switch_hostname></pre> <p>Note: This step takes 2-3 minutes to complete.</p> <p>The user is returned to the PMAC command prompt. If netConfig fails to complete successfully, contact Error! Bookmark not defined.</p> |
| <p>10. <input type="checkbox"/></p> | <p>Virtual PMAC: Validate XML file</p> | <p>This script validates the XML file to a limited extent. It verifies:</p> <ul style="list-style-type: none"> • The file is valid • All required options for commands are present • All provided options for commands are valid • SOME, but not all, option values <p>To validate the XML file:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig - file=6125XLG_configure.xml -testRun > dev/null</pre> <p>If nothing is returned then the XML file is valid to the extent defined above. Along with a brief description, errors return a string indicating the line location of the fault in the XML file.</p> |

Procedure 14. Configure HP 6125XLG Switch

| Step | Procedure | Result |
|---------------------------------|--|---|
| 11. <input type="checkbox"/> | Virtual PMAC: Configure the switch | <p>Configure the switch by issuing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- file=/usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml Processing file: /usr/TKLC/smac/etc/switch/xml/6125XLG_configure.xml</pre> <p>Note: This may take up to 2-3 minutes to complete.</p> <p>Check the output of this command for any errors. If this fails for any reason, stop this procedure and contact Error! Bookmark not defined.</p> <p>A successful completion of netConfig returns the user to the prompt.</p> |
| 12. <input type="checkbox"/> | Virtual PMAC: Add IPv6 default route (IPv6 network only) | <p>For IPv6 management networks, the enclosure switch requires an IPv6 default route to be configured. Apply the following command using netConfig:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addRoute network=::/0 nexthop=<mgmtVLAN_gateway_address></pre> |
| 13. <input type="checkbox"/> | Virtual PMAC: Verify proper configuration of switch | <p>Once the HP 6125G has finished booting from the previous step, verify network reachability and configuration.</p> <pre>\$ /bin/ping -w3 <enclosure_switch_IP> PING 10.240.8.10 (10.240.8.10) 56(84) bytes of data.64 bytes from 10.240.8.10: icmp_seq=1 ttl=255 time=0.637 ms64 bytes from 10.240.8.10: icmp_seq=2 ttl=255 time=0.661 ms64 bytes from 10.240.8.10: icmp_seq=3 ttl=255 time=0.732 m</pre> <pre>\$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP> <switch_platform_username>@<enclosure_switch_IP>'s password: <switch_platform_password> Switch_hostname> display current-configuration</pre> <p>Inspect the output and ensure it is configured as per site requirements.</p> |
| 14. <input type="checkbox"/> | Virtual PMAC | <p>For HP 6125XLG switches connected by 4x1GE LAG uplink perform Utility procedure 3.4.11 Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig); otherwise, for deployments with 10GE uplink, continue to the next step.</p> |
| 15. <input type="checkbox"/> | Virtual PMAC: Repeat | <p>Repeat steps 4. through 14. for each HP 6125XLG switch.</p> |
| 16. <input type="checkbox"/> | Virtual PMAC | <p>For HP 6125XLG switches linking with 4x1GE uplink to customer switches, field personnel are expected to work with the customer to set their downlinks to the HP 6125XLG 4x1GE LAG to match speed and duplex set in 14.</p> <p>For HP 6125XLG switches linking with 4x1GE LAG to product Cisco 4948/E/EF aggregation switches, perform Utility Procedure 3.4.12 Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig), to match speed and duplex settings from 14.</p> |
| 17. <input type="checkbox"/> | Virtual PMAC | <p>Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch for each switch configured in this procedure.</p> |

Procedure 14. Configure HP 6125XLG Switch

| Step | Procedure | Result |
|---------------------------------|--|---|
| 18. <input type="checkbox"/> | Virtual PMAC: Clean up FW file | Remove the FW file from the tftp directory. <pre>\$ sudo /bin/rm -f ~<switch_backup_user>/<FW_image></pre> |

3.3.6 Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch (netConfig)

This procedure configures a replacement HP switch.

Prerequisite: User has determined which switch has failed.

Procedure Reference Tables

Steps within this procedure may refer to variable data indicated by text within <>. Refer to this table for the proper value to insert depending on your system type. Fill in the appropriate value from [2] HP Solutions Firmware Upgrade Pack.

| Variable | Cisco 4948 | Cisco 4948E | Cisco 4948E-F |
|------------------|------------|-------------|---------------|
| <IOS_image_file> | | | |

Needed Material: HP MISC firmware ISO image

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

| Step | Procedure | Result |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Cabinet: Replace switch | Remove failed switch and replace with new switch of same model. |
| 2. <input type="checkbox"/> | Virtual PMAC: Move firmware image | Firmware version must be identical between mating switches, to check the firmware on the mate switch use the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=<switch_hostname> getFirmware</pre> Move the appropriate FW image from the switch backup directory to the TFTP directory by performing the following command: <pre>\$ sudo /bin/mv -i <switch_backup_directory>/<FW_image> ~<switch_backup_user>/</pre> Note: If the file does not exist on the server, copy it from the firmware media. <pre>\$ sudo /bin/chmod 644 <tftp_directory>/<FW_image></pre> |

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

| Step | Procedure | Result |
|--------------------------------|---|---|
| 3. <input type="checkbox"/> | Virtual PMAC: Initialize switch | For a 6120XG: Perform 3.3.3 Configure HP 6120XG Switch (netConfig), steps 3. -4. , 6. (init.xml only), and 8. Return to this procedure, and continue with the next step. For a 6125G: Perform 3.3.4 Configure HP 6125G Switch (netConfig), steps 3. -4. , 6. (init.xml only), and 8. Return to this procedure, and continue with the next step. For a 6125XLG: Perform 3.3.5 Configure HP 6125XLG Switch (netConfig), steps 3. , 4. -6. (init.xml only), and 8. Return to this procedure, and continue with the next step. |
| 4. <input type="checkbox"/> | Virtual PMAC: Copy switch backup file | Copy the switch backup files to the home directory of the <switch_backup_user> by performing the following command: <pre>\$ sudo /bin/cp -i /usr/TKLC/smac/etc/switch/backup/<switch_hostname>-backup* ~<switch_backup_user>/</pre> |
| 5. <input type="checkbox"/> | Virtual PMAC: Prepare to restore | <pre>\$ cd ~<switch_backup_user> \$ sudo /bin/chmod 644 ~<switch_backup_user>/<switch_hostname>-backup*</pre> |

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

| Step | Procedure | Result |
|--|---|---|
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC: Prepare to restore</p> | <p>Perform only if restoring a 6120XG switch; otherwise, skip to the next step. Some features enabled on a 6120XG may not restore properly if they reference a port channel that does not currently exist on the switch ahead of the restore operation. Identify any port channels that need to be created on the switch according to the backup file and create them before restoring the configuration:</p> <pre>\$ sudo /bin/cat <switch_hostname>-backup /bin/grep "^trunk"</pre> <p>Reference the following example:</p> <pre>\$ sudo /bin/cat <switch_hostname>-backup /bin/grep "^trunk" trunk <int list> Trk<id> LACP trunk <int list> Trk<id> Trunk</pre> <p>If any port-channels are found, then for each port channel identified by the above command, use the <code>netConfig setLinkAggregation</code> command to create it and the <code>netConfig showConfiguration</code> command to verify its configuration.</p> <p>For example, if an LACP port channel was found, add the port-channel by executing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation id=<id> addPort=tenGE<int list> mode=active</pre> <p>If a Trunk port-channel was found (as labeled after the Trk<id>), add the port channel by executing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 setLinkAggregation id=<id> addPort=tenGE<int list> mode=static</pre> <p>Verify the port-channels were added to the running configuration by executing the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY2 showConfiguration grep "^trunk" trunk <int list> Trk<id> LACP trunk <int list> Trk<id> Trunk</pre> |
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Restore</p> | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_hostname> restoreConfiguration service=ssh_service filename=<switch_hostname>-backup</pre> <p>Note: The switch reboots. It takes approximately 120-180 seconds before connectivity is restored.</p> |
| <p>8. <input type="checkbox"/></p> | <p>Cabinet: Attach cable to new switch</p> | <p>Connect all network and console cables to the new switch. Ensure each cable is connected to the same ports of the replacement switch as they were in the failed switch.</p> <p>Note: Refer to appropriate application schematic or procedure for determining which cables are used for customer uplink.</p> |

Procedure 15. Replace a Failed HP (6120XG, 6125G, 6125XLG) Switch

| Step | Procedure | Result |
|---------------------------------|---|---|
| 9. <input type="checkbox"/> | Virtual PMAC: Verify connectivity | For a 6120XG: Refer to 3.3.3 Configure HP 6120XG Switch (netConfig), steps 10. -12. Apply QoS policy and verify connectivity. For a 6125G: Refer to 3.3.4 Configure HP 6125G Switch (netConfig), step 17. For a 6125XLG: Refer to 3.3.5 Configure HP 6125XLG Switch (netConfig), step 11. |
| 10. <input type="checkbox"/> | Virtual PMAC: Clean up FW | Remove the FW images from the users' home directory and TFTP directory with the following command: <pre>\$ sudo rm ~admusr/<fw_filename> \$ sudo rm /var/TKLC/smac/image/<fw_filename></pre> |

3.4 Utility Procedures

3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch

Execute this procedure after every change to a switch configuration or after completing 3.3.3 Configure HP 6120XG Switch (netConfig), 3.3.4 Configure HP 6125G Switch (netConfig), or 3.3.5 Configure HP 6125XLG Switch (netConfig).

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Fill in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

| Variable | Value |
|--|--------|
| <switch_name> Hostname of switch | |
| <switch_backup_user> | admusr |
| <FW_image> FW file used in firmware upgrade/switch replacement/or initial install | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 16. Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch

| Step | Procedure | Result |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Target Server: Ensure directory exists | <pre>\$ sudo /bin/ls -i -l /usr/TKLC/smac/etc/switch/backup</pre> <p>If you receive an error such as the following:</p> <pre>-bash: ls: /usr/TKLC/smac/etc/switch/backup: No such file or directory</pre> <p>Then the directory must be created by issuing the following command:</p> <pre>\$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/switch/backup</pre> <p>Change the directory permissions:</p> <pre>\$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/switch/backup</pre> <p>Change directory ownership:</p> <pre>\$ sudo /bin/chown -R pmacd:pmacbackup /usr/TKLC/smac/etc/switch/backup</pre> |
| 2. <input type="checkbox"/> | Execute backup command | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> backupConfiguration service=ssh_service filename=<switch_name>-backup</pre> <p>Note: If the command failed with error message same as or similar to "Error saving to service", and the TPD version is 7.6.0.0.0_88.50.0 or later, please refer to Appendix T.</p> |
| 3. <input type="checkbox"/> | Copy files to backup directory | <pre>\$ sudo /bin/mv -i ~<switch_backup_user>/<switch_name>-backup* /usr/TKLC/smac/etc/switch/backup</pre> |
| 4. <input type="checkbox"/> | Verify | <p>Verify switch configuration was backed up by cat <switch_name> and inspect its contents to ensure it reflects the latest known good switch configurations.</p> <pre>\$ sudo /bin/ls -l /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup* ll P2-Switch1-backup* -rw-r----- 1 root root 11910 Jul 8 10:20 <switch_name>-backup -rw----- 1 admusr admgrp 69 Jul 8 10:20 <switch_name>-backup.info \$ sudo /bin/cat /usr/TKLC/smac/etc/switch/backup/<switch_name>-backup</pre> |
| 5. <input type="checkbox"/> | Repeat | Repeat steps 2. through 4. for each HP switch to back up. |
| 6. <input type="checkbox"/> | Virtual PMAC: Clean up FW | <p>Remove the FW images from the users' home directory and TFTP directory with the following command:</p> <pre>\$ sudo rm ~admusr/<fw_filename> \$ sudo rm /var/TKLC/smac/image/<fw_filename></pre> |

3.4.2 Configure SNMP Communities and Trap Servers

This procedure configures SNMP communities and trap servers.

Prerequisites:

It is essential that all switches have been configured successfully using:

- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and/or
- 3.3.1 Configure Cisco 3020 Switch (netConfig) and/or
- 3.3.3 Configure HP 6120XG Switch (netConfig) and/or
- 3.3.4 Configure HP 6125G Switch (netConfig) and/or
- 3.3.5 Configure HP 6125XLG Switch (netConfig) and/or

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Fill in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

| Variable | Value |
|---|-------|
| <switch_name> See Application Documentation and step 2. | |
| <switch_platform_username> See Application Documentation | |
| <community string> See Application Documentation | |
| <SNMP_server_IP> See Application Documentation | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 17. Configure SNMP Communities and Trap Servers

| Step | Procedure | Result |
|--------------------------------|-------------------------------|--------------------------|
| 1. <input type="checkbox"/> | Virtual PMAC: Login | Log into the PMAC Guest. |

Procedure 17. Configure SNMP Communities and Trap Servers

| Step | Procedure | Result |
|---|--|---|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC</p> | <p>1. Determine which devices require SNMP configuration.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices</pre> <p>Devices:</p> <p>Device: 6120XG_IOBAY3</p> <p>Vendor: HP</p> <p>Model: 6120</p> <p>Access: Network: 10.240.8.9</p> <p>Init Protocol Configured</p> <p>Live Protocol Configured</p> <p>Device: C3020_IOBAY1</p> <p>Vendor: Cisco</p> <p>Model: 3020</p> <p>Access: Network: 10.240.8.7</p> <p>Init Protocol Configured</p> <p>Live Protocol Configured</p> <p>Device: cClass-switch1A</p> <p>Vendor: Cisco</p> <p>Model: 4948E</p> <p>Access: Network: 10.240.8.3</p> <p>Access: OOB:</p> <p>Service: console_service</p> <p>Console: cClass-sw1A-console</p> <p>Init Protocol Configured</p> <p>Live Protocol Configured</p> <p>2. Determine which devices should have the community string added/removed.</p> <p>Refer to application documentation to determine which switches to add/remove the community string. Note the DEVICE NAME of each switch. This is used as <switch_name>. In the example output above, DEVICE NAME = 6120XG_IOBAY3, C3020_IOBAY1, and cClassswitch1A.</p> |
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC: Configure the community string</p> | <p>To ADD a community string:</p> <pre>\$sudo /usr/TKLC/plat/bin/netConfig addSNMP -- device=<switch_name> community=<community_string> uauth=RO</pre> <p>To DELETE a community string:</p> <pre>\$sudo /usr/TKLC/plat/bin/netConfig deleteSNMP -- device=<switch_name> community=<community_string></pre> |

Procedure 17. Configure SNMP Communities and Trap Servers

| Step | Procedure | Result |
|--|--|--|
| <p>4. <input type="checkbox"/></p> | <p>Virtual PMAC: Configure the SNMP trap server</p> | <p>To ADD a trap server:</p> <p>For the 6120XG:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig addSNMPNotify -- device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> traplvl=not-info</pre> <p>For all other devices:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig addSNMPNotify -- device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string></pre> <p>To DELETE a trap server:</p> <p>For the 6120XG:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig deleteSNMPNotify -- device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string> traplvl=not-info</pre> <p>For all other devices:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig deleteSNMPNotify -- device=<switch_name> host=<snmp_server_ip> version=2c auth=<community_string></pre> |
| <p>5. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify the SNMP configuration</p> | <p>Verify the switch has been configured with the appropriate SNMP communities and trap servers:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig getSNMP -- device=<switch_name> SNMP Community: "test" \$ sudo /usr/TKLC/plat/bin/netConfig listSNMPNotify -- device=<switch_name> Notification: = (Password change Login failures Port-Security Authorization Server Contact DHCP-Snooping Dynamic ARP Protection Dynamic IP Lockdown) Host: = (10.240.8.4 10.240.8.6)</pre> |
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC: Back up the switch configuration</p> | <p>For Cisco, perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig). For 6120XG, perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch.</p> |
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Repeat</p> | <p>Repeat steps 3. through 6. for each device.</p> |

3.4.3 Configure SNMPv3 Security Model and Trap Servers

This procedure configures SNMP Version 3 security model and trap servers. This SNMPv3 support is only for HP 6125G/XLG and Cisco 4948E/E-F switches.

Prerequisites:

It is essential that all switches have been configured successfully using:

- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and/or
- 3.3.4 Configure HP 6125G Switch (netConfig) and/or
- 3.3.5 Configure HP 6125XLG Switch (netConfig)

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Fill in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

| Variable | Value |
|---|-------|
| <switch_name> See Application Documentation and step 2. | |
| <switch_ip> See Application Documentation | |
| <SNMP_server_IP> See Application Documentation | |
| Security Level: (Can be single level or multiple levels for different groups and users) noAuthNoPriv, authNoPriv, AuthPriv | |
| noAuthNoPriv level: | |
| <noauth_group_name> | |
| < noauth_user_name> | |
| authNoPriv level: | |
| <auth_group_name> | |
| <auth_user_name> | |
| <auth_mode> md5, sha | |
| <auth_user_pass> | |
| AuthPriv level: | |
| <authpriv_group_name> | |
| <authpriv_user_name> | |
| < authpriv_auth_mode> md5, sha | |
| < authpriv_auth_pass> | |

| | |
|--|--|
| <p><priv_mode> 3des, aes, des for Cisco 4948E/EF switches 3des, aes128, des56 for HP 6125G/XLG switches.</p> | |
| <p><priv_word></p> | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 18. Configure SNMPv3 Security Model and Trap Servers

| Step | Procedure | Result |
|---|--|---|
| <p>1. <input type="checkbox"/></p> | <p>Virtual PMAC: Login</p> | <p>Log into the PMAC Guest.</p> |
| <p>2. <input type="checkbox"/></p> | <p>Virtual PMAC</p> | <p>3. Determine which devices require SNMP configuration.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices Devices: Device: 6125G_IOBAY5 Vendor: HP Model: 6120 Access: Network: 10.240.8.11 Init Protocol Configured Live Protocol Configured Device: 6125XLG_IOBAY6 Vendor: Cisco Model: 3020 Access: Network: 10.240.8.12 Init Protocol Configured Live Protocol Configured Device: cClass-switch1A Vendor: Cisco Model: 4948E Access: Network: 10.240.8.3 Access: OOB: Service: console_service Console: cClass-sw1A-console Init Protocol Configured Live Protocol Configured</pre> <p>4. Determine which devices should have the community string added/removed.</p> <p>Refer to application documentation to determine which switches to add/remove the community string. Note the DEVICE NAME of each switch. This is used as <switch_name>. In the example output above, DEVICE NAME = 6125G_IOBAY5, 6125XLG_IOBAY6, and cClassswitch1A.</p> |

Procedure 18. Configure SNMPv3 Security Model and Trap Servers

| Step | Procedure | Result |
|---|---|---|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC: Configure SNMPv3 level noAuthNoPriv</p> | <p>For Cisco 4948E/E-F:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server group <noauth_group_name> v3 noauth" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server user <noauth_user_name> <noauth_group_name> v3"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="snmp-server group mygroup1 v3 noauth" \$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="snmp-server user mynoauthUser mygroup1 v3"</pre> <p>For HP 6125G/XLG:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent group v3 <noauth_group_name>" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent usm-user v3 <noauth_user_name> <noauth_group_name>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent group v3 mygroup1" \$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent usm-user v3 mynoauthUser mygroup1"</pre> |
| <p>4.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC: Verify SNMPv3 level noAuthNoPriv</p> | <pre>\$ sudo snmpwalk -v 3 -u <noauth_user_name> -l noAuthNoPriv <switch_ip> <MIB object></pre> <p>Example Output:</p> <pre>\$ sudo snmpwalk -v 3 -u mynoauthUser -l noAuthNoPriv 10.240.8.12 iftable IF-MIB::ifIndex.2 = INTEGER: 2 IF-MIB::ifIndex.3 = INTEGER: 3</pre> |

Procedure 18. Configure SNMPv3 Security Model and Trap Servers

| Step | Procedure | Result |
|---|---|---|
| <p>5.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC: Configure SNMPv3 level authNoPriv</p> | <p>For Cisco 4948E/E-F:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server group <auth_group_name> v3 auth" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server user <auth_user_name> <auth_group_name> v3 auth <auth_mode> <auth_user_pass>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="snmp-server group mygroup2 v3 auth" \$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="snmp-server user myauthUser mygroup2 v3 auth md5 myauthPass"</pre> <p>For HP 6125G/XLG:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent group v3 <auth_group_name>" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent usm-user v3 <auth_user_name> <auth_group_name> authentication-mode <auth_mode> <auth_user_pass>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent group v3 mygroup2 authentication" \$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent usm-user v3 myauthUser mygroup2 simple authentication-mode md5 myauthPass"</pre> |
| <p>6.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC: Verify SNMPv3 level authNoPriv</p> | <pre>\$ sudo snmpwalk -v 3 -u <auth_user_name> -l authNoPriv -A <auth_user_pass> <switch_ip> <MIB object></pre> <p>Example Output:</p> <pre>\$ sudo snmpwalk -v 3 -u mynoauthUser -l authNoPriv -A myauthPass 10.240.8.12 iftable IF-MIB::ifIndex.2 = INTEGER: 2 IF-MIB::ifIndex.3 = INTEGER: 3 ...</pre> |

Procedure 18. Configure SNMPv3 Security Model and Trap Servers

| Step | Procedure | Result |
|---|---|---|
| <p>7.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC: Configure SNMPv3 level AuthPriv</p> | <p>For Cisco 4948E/E-F:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server group <authpriv_group_name> v3 priv" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server user <authpriv_user_name> <authpriv_group_name> v3 auth <authpriv_auth_mode> <authpriv_user_pass> priv <priv_mode> <priv_word>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="snmp-server group mygroup3 v3 priv" \$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="snmp-server user myprivUser mygroup3 v3 auth md5 myprivPass priv des myprivWord"</pre> <p>For HP 6125G/XLG:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent group v3 <auth_group_name>" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent usm-user v3 <auth_user_name> <auth_group_name>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent group v3 mygroup3 privacy" \$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent usm-user v3 myprivUser mygroup3 simple authentication-mode md5 myprivPass privacy-mode des56 myprivWord" - "simple" only for 6125XLG \$ sudo /usr/TKLC/plat/bin/netConfig --device=6125G_IOBAY5 userConfigureCommand command="snmp-agent usm-user v3 myprivUser mygroup3 authentication-mode md5 myprivPass privacy-mode des56 myprivWord" - no "simple" for 6125G</pre> |
| <p>8.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC: Verify SNMPv3 level AuthPriv</p> | <pre>\$ sudo snmpwalk -v 3 -u <authpriv_user_name> -l AuthPriv - a MD5 -A <authpriv_user_pass> -x DES -X <priv_word> <switch_ip> <MIB object></pre> <p>Example Output:</p> <pre>\$ sudo snmpwalk -v 3 -u myprivUser -l AuthPriv -a MD5 -A myprivPass -x DES -X myprivWord 10.240.8.12 iftable IF-MIB::ifIndex.2 = INTEGER: 2 IF-MIB::ifIndex.3 = INTEGER: 3</pre> |

Procedure 18. Configure SNMPv3 Security Model and Trap Servers

| Step | Procedure | Result |
|------------------------------------|--|--|
| <p>9. <input type="checkbox"/></p> | <p>Virtual PMAC: Configure the SNMPv3 trap server</p> | <p>To ADD a SNMPv3 trap server, the <noauth_user_name>, <auth_user_name>, <authpriv_user_name> have to be configured in the previous steps.</p> <p>For the Cisco 4948E/E-F switches:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command=" snmp-server host <snmp_server_ip> version 3 noauth <noauth_user_name>"</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command=" snmp-server host <snmp_server_ip> version 3 auth <auth_user_name>"</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command=" snmp-server host <snmp_server_ip> version 3 priv <authpriv_user_name>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command=" snmp-server host 176.16.1.100 version 3 noauth mynoauthUser"</pre> <p>For 6125G/XLG switches:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent target-host trap address udp-domain <snmp_server_ip> params securityname <noauth_user_name> v3"</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server host <snmp_server_ip> params securityname <auth_user_name> v3 authentication"</pre> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server host <snmp_server_ip> params securityname <authpriv_user_name> v3 privacy"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent target-host trap address udp-domain 176.16.1.100 params securityname myauthUser v3 authentication"</pre> |

Procedure 18. Configure SNMPv3 Security Model and Trap Servers

| Step | Procedure | Result |
|---------------------------------|---|---|
| 10. <input type="checkbox"/> | Virtual PMAC: Verify the SNMPv3 trap server | From the trap server, run tcpdump to watch the trap packets which come from the switches, see the packets are encrypted with AuthPriv user. \$ sudo tcpdump -i management port 162 |
| 11. <input type="checkbox"/> | Virtual PMAC: Delete the SNMPv3 trap server | To DELETE a SNMPv3 trap server: For Cisco 4948E/E-F switches: Run the userConfigureCommand from the Step 17 whole commands appended with "no". Example: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="no snmp-server host 176.16.1.100 version 3 noauth mynoauthUser"</pre> For 6125G/XLG switches, run the userConfigureCommand appended with "undo" but end after securityname <user_name> Example: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="undo snmp-agent target-host trap address udp-domain 10.75.207.101 params securityname myauthUser"</pre> |

3.4.4 Configure Access List to only allow specific IP to use SNMPv2 community String

Due to the SNMPv3 configuration to have more secure SNMP access, the SNMPv2 should be denied. Some Management Server(s) still reply on SNMPv2 for some applications, they request SNMPv2 access. Access list is configured on switches to allow specific IPs to use SNMPv2 community string.

This procedure configures Access List on 6125G/XLG and Cisco 4948E/EF switches for the above purpose.

Prerequisites:

It is essential that all switches have been configured successfully using:

- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and/or
- 3.3.4 Configure HP 6125G Switch (netConfig) and/or
- 3.3.5 Configure HP 6125XLG Switch (netConfig)

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Fill in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

| Variable | Value |
|---|-------|
| <switch_name> See Application Documentation and step 2. | |
| <switch_ip> See Application Documentation | |
| <community_string> See Application Documentation | |
| <access_list_number> 1-99 for basic ACL on 4948E/E-F 2000-2999 for basic ACL on 6125G/XLG | |

Procedure 19. Configure Access List to allow specific IP to access SNMPv2

| Step | Procedure | Result |
|--------------------------------|-------------------------------|--------------------------|
| 1. <input type="checkbox"/> | Virtual PMAC: Login | Log into the PMAC Guest. |

Procedure 19. Configure Access List to allow specific IP to access SNMPv2

| Step | Procedure | Result |
|---|----------------------------|--|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC</p> | <p>5. Determine which devices require SNMP configuration.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices</pre> <p>Devices:</p> <p>Device: 6125G_IOBAY5</p> <p>Vendor: HP</p> <p>Model: 6120</p> <p>Access: Network: 10.240.8.11</p> <p>Init Protocol Configured</p> <p>Live Protocol Configured</p> <p>Device: 6125XLG_IOBAY6</p> <p>Vendor: Cisco</p> <p>Model: 3020</p> <p>Access: Network: 10.240.8.12</p> <p>Init Protocol Configured</p> <p>Live Protocol Configured</p> <p>Device: cClass-switch1A</p> <p>Vendor: Cisco</p> <p>Model: 4948E</p> <p>Access: Network: 10.240.8.3</p> <p>Access: OOB:</p> <p>Service: console_service</p> <p>Console: cClass-sw1A-console</p> <p>Init Protocol Configured</p> <p>Live Protocol Configured</p> <p>6. Determine which devices to configure the access-list.</p> <p>Refer to application documentation to determine which switches to configure the access-list to allow access SNMPv2 with the community string. Note the DEVICE NAME of each switch. This is used as <switch_name>. In the example output above, DEVICE NAME = 6125G_IOBAY5, 6125XLG_IOBAY6, and cClassswitch1A.</p> |

Procedure 19. Configure Access List to allow specific IP to access SNMPv2

| Step | Procedure | Result |
|---|--|--|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Virtual PMAC:</p> <p>Configure Access List</p> | <p>For Cisco 4948E/E-F:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="access-list <access_list_number> permit <server_ip>" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="access-list <access_list_number> deny any" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-server community <community_string> <access_list_number>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="access-list 1 permit 176.16.1.100" \$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="access-list 1 deny any" \$ sudo /usr/TKLC/plat/bin/netConfig --device=cClass_switch1A userConfigureCommand command="snmp-server community tklcComm 1"</pre> <p>For HP 6125G/XLG:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="acl number <access_list_number>" commandPrompt="acl-basic" subcommand="rule permit source <server_ip> 0" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="acl number <access_list_number>" commandPrompt="acl-basic" subcommand="rule deny source any" \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> userConfigureCommand command="snmp-agent community read <community_string> acl <access_list_number>"</pre> <p>Example:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="acl number 2000" commandPrompt="acl-basic" subcommand="rule permit source 10.240.8.100 0" \$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="acl number 2000" commandPrompt="acl-basic" subcommand="rule deny source any" \$ sudo /usr/TKLC/plat/bin/netConfig --device=6125XLG_IOBAY6 userConfigureCommand command="snmp-agent community read tklcComm acl 2000"</pre> |

Procedure 19. Configure Access List to allow specific IP to access SNMPv2

| Step | Procedure | Result |
|--------------------------------|---|---|
| 4. <input type="checkbox"/> | From permitted <server_ip>:: Verify only the specific IP can access SNMPv2 with the community string. | <pre>\$ sudo snmpwalk -v2c -c<community_string> <switch_ip> <MIB object></pre> Example Output: <pre>\$ sudo snmpwalk -v2c -ctklcComm 10.240.8.12 iftable IF-MIB::ifIndex.2 = INTEGER: 2 IF-MIB::ifIndex.3 = INTEGER: 3</pre> |
| 5. <input type="checkbox"/> | From other servers: Can't access the SNMPv2 | <pre>\$ sudo snmpwalk -v2c -c<community_string> <switch_ip> <MIB object></pre> Example Output: <pre>\$ sudo snmpwalk -v2c -ctklcComm 10.240.8.12 iftable Timeout: No Response from 10.240.8.12</pre> |

3.4.5 Configure QoS (DSCP and/or CoS) on HP 6120XG Switches

This procedure configures QoS on HP 6120XG switches.

Prerequisites:

It is essential that all switches have been configured successfully using:

- 3.3.3 Configure HP 6120XG Switch (netConfig)

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Refer back to this table for the proper value to insert depending on your system type.

| Variable | Value |
|--|-------|
| <switch_name> See Application Documentation and step 2. | |
| <dscp value> See Application Documentation (if available) | |
| <cos value> See Application Documentation (if available) | |
| <switch_platform_username> See Application Documentation | |
| <VLANID> See Application Documentation | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 20. Configure QoS (DSCP and/or CoS) on HP 6120XG Switches

| Step | Procedure | Result |
|--------------------------------|-------------------------------|---|
| 1. <input type="checkbox"/> | Virtual PMAC: Login | Log into the PMAC Guest. |
| 2. <input type="checkbox"/> | Virtual PMAC | <p>1. Determine which devices require QoS policies.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices Devices: Device: 6120XG_IOBAY3 Vendor: HP Model: 6120 Access: Network: 10.240.8.9 Init Protocol Configured Live Protocol Configured Device: C3020_IOBAY1 Vendor: Cisco Model: 3020 Access: Network: 10.240.8.7 Init Protocol Configured Live Protocol Configured Device: cClass-switch1A Vendor: Cisco Model: 4948E Access: Network: 10.240.8.3 Access: OOB: Service: console_service Console: cClass-sw1A-console Init Protocol Configured Live Protocol Configured</pre> <p>2. Determine which devices should have the community string added/removed.</p> <p>Refer to application documentation to determine which switches or pairs of switches to configure with QoS.. Note the DEVICE NAME of each 6120XG switch. This is used as <switch_name>. In the example output above, DEVICE NAME = 6120XG_IOBAY3, C3020_IOBAY1, and cClassswitch1A.</p> |

Procedure 20. Configure QoS (DSCP and/or CoS) on HP 6120XG Switches

| Step | Procedure | Result |
|--------------------------------|--|--|
| 3. <input type="checkbox"/> | Virtual PMAC: Add DSCP and/or CoS policy | Configure DSCP and/or CoS marking on the device. For DSCP and CoS Marking: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig addQoS -- device=<switch_name> vlan=<vlanid> dscp=<dscp value> cos=<cos value> name=<user defined name></pre> For DSCP Marking Only: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig addQoS -- device=<switch_name> vlan=<vlanid> dscp=<dscp value> name=<user defined name></pre> For CoS Marking Only: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig addQoS -- device=<switch_name> vlan=<vlanid> cos=<cos value></pre> |
| 4. <input type="checkbox"/> | Virtual PMAC: Verify QoS configuration | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig getQoS -- device=<switch_name> vlan=<vlanid></pre> Example Output: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig getQoS -- device=6120XG_IOBAY3 vlan=2 Policy: = (VLAN priorities VLAN ID Apply rule DSCP Priority 2 DSCP 000011 3)</pre> |
| 5. <input type="checkbox"/> | Virtual PMAC: Repeat | Repeat steps 3. through 4. for each policy that needs to be applied to the switch. |
| 6. <input type="checkbox"/> | Virtual PMAC: Back up the switch configuration | Perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch. |
| 7. <input type="checkbox"/> | Virtual PMAC: Repeat | Repeat steps 3. through 6. for each switch. |

3.4.6 Configure Port Mirroring

This procedure configures port mirroring.

Prerequisites:

It is essential that all switches have been configured successfully using:

- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and/or
- 3.3.1 Configure Cisco 3020 Switch (netConfig) and/or
- 3.3.3 Configure HP 6120XG Switch (netConfig) and/or
- 3.3.4 Configure HP 6125G Switch (netConfig) and/or
- 3.3.5 Configure HP 6125XLG Switch (netConfig) and/or

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Refer back to this table for the proper value to insert depending on your system type.

| Variable | Value |
|---|-------|
| <switch_name> See Application Documentation and step 2. | |
| <switch_model> Value from step 2. | |
| <switch_IP> Value from step 2. | |
| <srcInterface> See Application Documentation | |
| <destInterface> See Application Documentation | |
| <switch_platform_username> See Application Documentation | |
| <srcVLANID> See Application Documentation | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 21. Configure Port Mirroring

| Step | Procedure | Result |
|--------------------------------|-------------------------------|---|
| 1. <input type="checkbox"/> | Virtual PMAC: Login | Log into the PMAC Guest. |
| 2. <input type="checkbox"/> | Virtual PMAC | <p>1. Determine which devices require port mirroring configuration.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices Devices: Device: 6120XG_IOBAY3 Vendor: HP Model: 6120 Access: Network: 10.240.8.9 Init Protocol Configured Live Protocol Configured Device: C3020_IOBAY1 Vendor: Cisco Model: 3020 Access: Network: 10.240.8.7 Init Protocol Configured Live Protocol Configured Device: 6125G_IOBAY5 Vendor: HP</pre> |

Procedure 21. Configure Port Mirroring

| Step | Procedure | Result |
|------------------------------------|--|---|
| | | <pre> Model: 6125 Access: Network: 10.240.8.12 Access: OOB: Service: oa_service Console: 5 Init Protocol Configured Live Protocol Configured Device: cClass-switch1A Vendor: Cisco Model: 4948E Access: Network: 10.240.8.3 Access: OOB: Service: console_service Console: cClass-sw1A-console Init Protocol Configured Live Protocol Configured </pre> <p>2. Determine which devices should have the community string added/removed.</p> <p>Refer to application documentation to determine which switches to add/remove the community string. Note the DEVICE NAME, MODEL, and IP ADDRESS of each switch. These are used as <switch_name>, <switch_model>, and <switch_IP>.</p> |
| <p>3. <input type="checkbox"/></p> | <p>Virtual PMAC: Configure port mirroring</p> | <p>For VLAN Monitoring (Cisco Devices Only):</p> <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addPortMirrorSession=1 vlan=<srcVlanid> destInterface=<mirrorPort> direction=both </pre> <p>For Port Mirroring:</p> <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --device=<switch_name> addPortMirrorSession=1 sourceInterface=<srcInterface> destInterface=<mirrorPort> direction=both </pre> <p>Notes:</p> <ul style="list-style-type: none"> • The interface option allows for more than one source interface. The value can be entered as a single interface, for example, GE1 (1Gb port) or tenGE1 (10Gb port) or it can be entered as a range of interfaces separated by commas and dashes, for example, GE1-5,GE7,tenGE9-10. • The only direction supported by the HP switches is both. If the direction option is used on an HP switch, it is ignored and both is applied. <p>VLAN Example:</p> <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --device=C3020_IOBAY1 addPortMirrorSession=1 vlan=2 destInterface=GE10 direction=both </pre> <p>Port Example:</p> <pre> \$ sudo /usr/TKLC/plat/bin/netConfig --device=6120XG_IOBAY3 addPortMirrorSession=1 sourceInterface=tenGE1,tenGE3 destInterface=tenGE2 </pre> |

Procedure 21. Configure Port Mirroring

| Step | Procedure | Result |
|--------------------------------|---|---|
| 4. <input type="checkbox"/> | Virtual PMAC: Verify port mirroring configuration | <pre>\$ sudo /usr/TKLC/plat/bin/netConfig getPortMirror session=1 -- device=6120XG_IOBAY3 Session: 1 Direction: both Source: tenGE2 Destination: tenGE1,tenGE3 \$ sudo /usr/TKLC/plat/bin/netConfig getPortMirror session=1 -- device=6125G_IOBAY4 Session: 1 Direction: both Source: GE1 Destination: GE22</pre> <p>Note: Output from the command may vary slightly from one device type to another.</p> |
| 5. <input type="checkbox"/> | Virtual PMAC: Back up the switch configuration | <p>For Cisco, perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig). For HP, perform 3.4.1 Back Up HP (6120XG, 6125G, 6125XLG) or Cisco 9372TX-E Switch.</p> |
| 6. <input type="checkbox"/> | Virtual PMAC: Repeat | Repeat steps 3. through 5. for each device. |

3.4.7 SwitchConfig to netConfig Repository Configuration

This procedure configures the netConfig repository with the necessary services and previously configured switches from a single management server for use with the c-Class platform.

Prerequisites:

- 8.1 IPM Management Server
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest
- 9.4 Set Up PMAC
- Application management network interfaces must be configured on the management servers before executing this procedure.
- Application username and password for creating switch backups must be configured on the management server before executing this procedure.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Refer back to this table for the proper value to insert depending on your system type.

| Variable | Value |
|--|---------------|
| <serial console type> | U=USB, c=PCIe |
| <switch_hostname> From NAPD or output from <code>listDevices</code> command | |
| <switch_platform_username> See Application Documentation | |
| <switch_platform_password> See referring application documentation | |
| <switch_console_password> See referring application documentation | |
| <switch_enable_password> See referring application documentation | |
| <management_server1A_mgmtVLAN_IP_address> | |
| <management_server1B_mgmtVLAN_IP_address> | |
| <PMAC_mgmtVLAN_IP_address> | |
| <switch_mgmtVLANID> | |
| <switch1A_mgmtVLAN_IP_address> | |
| <switch1B_mgmtVLAN_IP_address> | |
| <mgmt_VLAN_subnet_ID> | |
| <netmask> | |
| <switch_Internal_VLAN_list> | |
| <management_server1A_iLO_IP> | |
| <management_server1B_iLO_IP> | |
| <platcfg_password> Initial password as provided by Oracle | |
| <management_server_mgmtInterface> Value gathered from NAPD | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> Check application documentation | |

Notes:

- The onboard administrators are not available during the configuration of Cisco 4948/4948E/4948E-F switches.

- Uplinks must be disconnected from the customer network before executing this procedure. One of the steps in this procedure describes when to reconnect these uplink cables. Refer to the application appropriate schematic or procedure for determining which cables are used for customer uplink.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Management Server iLO: Login and start the integrated remote console | <ol style="list-style-type: none"> 1. On Server1A, log into iLO with Internet Explorer using the password provided by the application: <code>http://<management_server1A_iLO_IP></code> 2. Click the Remote Console tab and start the Integrated Remote Console on the server. 3. If the Security Alert displays, click Yes. 4. If not already done so, login as admusr. |
| 2. <input type="checkbox"/> | Management Server: Pre-check. Verify hardware type | <p>Certain steps in this procedure require enabling and disabling ethernet interfaces. This procedure supports DL360 and DL380 servers. The interfaces that are to be enabled and disabled are different for each server type.</p> <p>To determine the interface name, on the server, execute the following command:</p> <pre>\$ /bin/cat /proc/net/bonding/bond0 grep Interface Slave Interface: eth01 Slave Interface: eth02</pre> <p>Note the slave interface names of ethernet interfaces to use in subsequent steps. The first line is the value for <ethernet_interface_1> and the second line is the value for <ethernet_interface_2> .</p> <p>For example, from the sample output provided, <ethernet_interface_1> is eth01. If the output from the above command is not successful, refer back to the application documentation.</p> |
| 3. <input type="checkbox"/> | Management Server: Pre-check. Determine platform version | <p>On each management server, determine the platform version of the system by issuing the following command:</p> <pre>\$ /usr/TKLC/plat/bin/appRev</pre> <p>If the following is shown in the output, the platform version is 7.2: Base Distro Release: 7.2.x.x.x_x.x.x</p> <p>The values of x-x.x.x do not matter. The value of 7.2 shows the platform version. If the command shows a Base Distro Release version lower than 7.2, or fails to execute, stop this procedure and refer back to application procedures. It is possible the wrong version of TVOE/TPD is installed.</p> |
| 4. <input type="checkbox"/> | Management Server: Pre-check. Verify virtual PMAC is installed | <ol style="list-style-type: none"> 1. Verify virtual PMAC installation by issuing the following commands as admusr on the management server: <pre>\$ sudo /usr/bin/virsh list --all Id Name State 6 vm-pmac1A running</pre> 2. If this command provides no output, it is likely that a virtual instance of PMAC is not installed. Refer to application documentation or Error! Bookmark not defined. |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|-----------------|--|--|
| <p>5. □</p> | <p>Virtual PMAC: Run conserverSetup command</p> | <pre>\$ sudo /usr/TKLC/plat/bin/conserverSetup -<serial console type> -s <management_server_mgmt_ip_address></pre> <p>You are asked for the platcfg credentials. An example:</p> <pre>[admusr@vm-pmac1A]\$ sudo /usr/TKLC/plat/bin/conserverSetup - u -s <management_server_mgmt_ip_address> Enter your platcfg username, followed by [ENTER]:platcfg Enter your platcfg password, followed by [ENTER]:<platcfg_password> Checking Platform Revision for local TPD installation... The local machine is running: Product Name: PMAC Base Distro Release: 7.2.0.0.0_88.6.0 Checking Platform Revision for remote TPD installation... The remote machine is running: Product Name: TVOE Base Distro Release: 7.2.0.0.0_88.6.0 Configuring switch 'switch1A_console' console server...Configured. Configuring switch 'switchBA_console' console server...Configured. Configuring iptables for port(s) 782...Configured. Configuring iptables for port(s) 1024:65535...Configured. Configuring console repository service... Repo entry for "console_service" already exists; deleting entry for: Service Name: console_service Type: conserver Host: <management_server_mgmt_ip_address> ...Configured. Slave interfaces for bond0: bond0 interface: eth01 bond0 interface: eth02</pre> <p>If this command fails, contact Error! Bookmark not defined.. Verify the output of the script. Verify your product release is based on Platform 7.2 (versions 7.2.x.x.x_x.x.x). Note the slave interface names of bond interfaces (<ethernet_interface_1> and <ethernet_interface_2>) for use in subsequent steps.</p> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|--|--|--|
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC: Log into the console of the virtual PMAC</p> | <p>Note: On a TVOE host, if you open the virsh console, for example, <code>\$ sudo /usr/bin/virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or the output is not correct, then there is likely a stuck virsh console command already being run on the TVOE host. Exit out of the virsh console, run <code>ps -ef grep virsh</code>, and then kill the existing process <code>kill -9 <PID></code>. Then execute the <code>virsh console X</code> command. Your console session should now run as expected.</p> <p>From management server1A, log into the console of the virtual PMAC.</p> <pre>\$ sudo /usr/bin/virsh console vm-pmac1A Connected to domain vm-pmac1A Escape character is ^] <Press ENTER key> CentOS release 6.2 (Final) Kernel 2.6.32-220.7.1.el6prere16.0.0_80.13.0.x86_64 on an x86_64</pre> <p>If another user is already logged in, logout and log back in as admusr.</p> <pre>[root@pmac ~]\$ logout vm-pmac1A login: admusr Password: Last login: Fri May 25 16:39:04 on ttyS4</pre> <p>If this command fails, it is likely that a virtual instance of PMAC is not installed. Refer to application documentation or contact Error! Bookmark not defined.</p> |
| <p>7. <input type="checkbox"/></p> | <p>Virtual PMAC: Verify PMAC release version</p> | <pre>\$ /usr/TKLC/plat/bin/appRev</pre> <p>If the following is shown in the output, the PMAC version is 5.0:</p> <pre>Product Name: PMAC Product Release: 5.0.0_x.x.x</pre> <p>If the output does not contain Product Name: PMAC or does not contain a PMAC version of 5.0 or higher, then stop this procedure and refer back to the application instructions.</p> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|-----------------|---|--|
| <p>8. □</p> | <p>Virtual PMAC: Set up netConfig repository with TFTP information</p> | <p>Use netConfig to create a repository entry that uses the tftp service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=tftp_service Service type? [dhcp, oa, oobm, ssh, tftp, conserver] tftp TFTP host IP? <pmac_mgmtVLAN_IP_address> Directory on host? /var/TKLC/smac/image/ Add service for tftp_service successful</pre> <p>To make sure you entered the information correctly, use the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=tftp_service</pre> <p>Check the output, which is similar to the one shown below.</p> <p>Note: Only the TFTP service information has been shown in this example. If the previous step and this step were done correctly, both the console_service and tftp_service entries would show up.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=tftp_service Services: Service Name: tftp_service Type: tftp Host: 10.240.8.4 Options: dir: /var/TKLC/smac/image</pre> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|---|---|--|
| <p>9. <input type="checkbox"/></p> | <p>Virtual PMAC: Set up netConfig repository with ssh information</p> | <p>1. Use netConfig to create a repository entry that uses the ssh service. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addService name=ssh_service Service type? (tftp, ssh, conserver, oa) ssh Service host? <PMAC_mgmtVLAN_IP_address> SSH password: <switch_backup_user_password> Verify Password: <switch_backup_user_password> Add service for ssh_service successful</pre> <p>2. To ensure you entered the information correctly, use the following command and inspect the output, which is similar to the one shown below.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo showService name=ssh_service Service Name: ssh_service Type: ssh Host: 10.250.8.4 Options: password: C20F7D639AE7E7 user: admusr</pre> |
| <p>10. <input type="checkbox"/></p> | <p>Virtual PMAC: Set up netConfig repository with aggregation switch information</p> | <p>Note: If there are no new aggregation switches to be configured, go to the next step.</p> <p>Use netConfig to create a repository entry for each switch. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <p>Note: The <device_model> can be 4948, 4948E, or 4948E-F depending on the model of the device. If you do not know, stop now and contact Error! Bookmark not defined..</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? Cisco Device Model [3020, 4948, 4948E,4948E-F]? <device_model> What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>/prefix Is the management interface a port or a vlan? [vlan]: [Enter] What is the VLAN ID of the management VLAN? [2]: [mgmt_vlanID] What is the name of the management VLAN? [management]: [Enter] What switchport connects to the management server? [GE40]: [Enter]</pre> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|------|-----------|--|
| | | <pre> What is the switchport mode (access trunk) for the management server port? [trunk]: [Enter] What are the allowed vlans for the management server port? [1,2]: <control_vlanID>, <mgmt_vlanID> Enter the name of the firmware file [cat4500e-entservicesk9- mz.122-54.XO.bin]: <IOS_filename> Firmware file to be used in upgrade: <IOS_filename> Enter the name of the upgrade file transfer service: tftp_service File transfer service to be used in upgrade: tftp_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? console_service What is the name of the console for OOB access? <console name> What is the platform access username? <switch_platform_username> What is the device console password? <switch_console_password> Verify password: <switch_console_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_enable_password> Verify password: <switch_enable_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_IP_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: console_service Device named <switch_hostname> successfully added. To check you entered the information correctly, use the following command: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=switch1A and check the output, which is similar to the one shown: \$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices Device: switch1A Vendor: Cisco Model: 4948E Access: Network: 10.240.64.34 Access: OOB: </pre> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|---|---|--|
| | | <pre>Service: console_service Console: switch1A_console Init Protocol Configured Live Protocol Configured</pre> |
| <p>11. <input type="checkbox"/></p> | <p>Virtual PMAC: Set up netConfig repository with switch information</p> | <p>Notes:</p> <ul style="list-style-type: none"> • If there are no new 3020s to be configured, go to the next step. • The Cisco 3020 is not compatible with IPv6 management configuration. <p>Use netConfig to create a repository entry for each 3020. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> • If you do not know any of the required answers, stop now and contact Error! Bookmark not defined. • The device name must be 20 characters or less. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? Cisco Device Model [3020, 4948, 4948E,4948E-F]? 3020 What is the management address? <enclosure_switch_ip> Enter the name of the firmware file [cbs30x0-ipbasek9-tar.122-58.SE1.tar]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service: <tftp_service> File transfer service to be used in the upgrade: <tftp_service> Should the init network adapter be added (y/n)? y Adding netBootInit protocol for <switch_hostname> using network... Network device access already set: <enclosure_switch_ip> What is the platform access username? <switch_platform_username> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_enable_password> Verify password: <switch_enable_password> Should the init file adapter be added (y/n)? y Adding netBootInit protocol for <switch_hostname> using file... What is the name of the service used for TFTP access? tftp_service</pre> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|---|---|---|
| | | <pre>Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <enclosure_switch_ip> Device named <switch_hostname> successfully added. To check you entered the information correctly, use the following command: \$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices and check the output, which is similar to the one shown below. \$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices Devices: Device: C3020_IOBAY1 Vendor: Cisco Model: 3020 Access: Network: 10.240.8.7Init Protocol Configured Live Protocol Configured Repeat this step for each 3020, using appropriate values for those 3020s. Note: If you receive the WARNING below, it means the <FW_image> is not found in the directory named in the FW Service. or the ssh_service, it is the user's home directory. For tftp_service, it is normally /var/TKLC/smac/ image: WARNING: Could not find firmware file on local host. If using a local service, please update the device entry using the editDevice command or copy the file to the correct location.</pre> |
| <p>12. <input type="checkbox"/></p> | <p>Virtual PMAC: Set up netConfig repository with HP 6120XG switch information</p> | <p>Note: If there are no 6120XGs to be configured, stop and continue with the appropriate switch configuration procedure.</p> <p>Use netConfig to create a repository entry for each 6120XG. This command provides the user with several prompts. The prompts shown with <variables> as the answers are site specific that the user MUST modify. Other prompts that do not have a <variable> shown as the answer must be entered EXACTLY as they are shown here.</p> <ul style="list-style-type: none"> • If you do not know any of the required answers, stop now and contact Error! Bookmark not defined.. • The device name must be 20 characters or less. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo addDevice name=<switch_hostname> --reuseCredentials Device Vendor? HP Device Model? 6120 What is the IPv4 (CIDR notation) or IPv6 (address/prefix notation) address for management?: <switch_mgmt_IP_address>/prefix Enter the name of the firmware file [Z_14_37.swi]: <FW_image> Firmware file to be used in upgrade: <FW_image> Enter the name of the upgrade file transfer service:</pre> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|------|-----------|---|
| | | <pre>ssh_service File transfer service to be used in upgrade: ssh_service Should the init oob adapter be added (y/n)? y Adding consoleInit protocol for <switch_hostname> using oob... What is the name of the service used for OOB access? oa_service_en<enclosure #> What is the name of the console for OOB access? <io_bay> What is the platform access username? <switch_platform_username> What is the device console password? <switch_platform_password> Verify password: <switch_platform_password> What is the platform user password? <switch_platform_password> Verify password: <switch_platform_password> What is the device privileged mode password? <switch_platform_password> Verify password: <switch_platform_password> Should the live network adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using network... Network device access already set: <switch_mgmt_IP_address> Should the live oob adapter be added (y/n)? y Adding cli protocol for <switch_hostname> using oob... OOB device access already set: oa_service_en<enclosure #> Device named <switch_hostname> successfully added The image is being unpacked and validated. This takes approximately 4 minutes. Once the unpacking, validation, and rebooting have completed, you are returned to the normal prompt. Proceed with the next step. To verify you entered the information correctly, use the following command: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> and check the output, which is similar to the one shown: \$ sudo /usr/TKLC/plat/bin/netConfig --repo showDevice name=<switch_hostname> Device: 6120XG_IOBAY1 Vendor: HP Model: 6120 FW Ver: 0 Access: Network: 10.240.8.10 Init Protocol Configured Live Protocol Configured Repeat this step for each 6120, using appropriate values for those 6120s.</pre> |

Procedure 22. SwitchConfig to netConfig Repository Configuration

| Step | Procedure | Results |
|---------------------------------|-----------------------------------|---|
| 13. <input type="checkbox"/> | Virtual PMAC: Migration | Perform the Procedure 23 Cisco Switch SwitchConfig to netConfig Migration procedure for all switches in the system. |

3.4.8 Cisco Switch SwitchConfig to netConfig Migration

This procedure configures Cisco switch to migrate from switchConfig to netConfig.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Refer back to these tables for the proper value to insert depending on your system type.

| Variable | Serial Port |
|------------------------|-------------|
| <switch1A_serial_port> | ttyS4 |
| <switch1B_serial_port> | ttyS5 |

Fill in the blanks with values for this site.

| Variable | Value |
|---|-------|
| <switch_platform_username> | |
| <switch_platform_password> See referring application documentation | |
| <switch_console_password> See referring application documentation | |
| <switch_enable_password> See referring application documentation | |
| <PMAC_mgmtVLAN_IP_address> | |
| <switch_mgmtVLAN_ID> | |
| <mgmt_VLAN_subnet_ID> | |
| <netmask> | |
| <switch_internal_VLAN_list> | |
| <management_server1A_iLO_IP> | |
| <management_server1B_iLO_IP> | |
| <switch_mgmt_IP_address> | |

| Variable | Value |
|--|--------|
| <platcfg_password> Initial password as provided by Oracle | |
| <management_server_mgmtInterface> Value gathered from NAPD | |
| <switch_backup_user> | admusr |
| <switch_backup_user_password> Check application documentation | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 23. Cisco Switch SwitchConfig to netConfig Migration

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Virtual PMAC: Verify network connectivity to the switch | <code>\$ /bin/ping -w3 <switch_mgmt_IP_address></code> |
| 2. <input type="checkbox"/> | Virtual PMAC: Login | Log into the switch using Telnet. <code>\$ /usr/bin/telnet <switch_mgmt_IP_address></code> |
| 3. <input type="checkbox"/> | Switch CLI: Apply netConfig commands | From the switch CLI, apply the following commands required by netConfig: <pre>Switch# config Switch(config)# hostname <switch_name> Switch(config)# no service config Switch(config)# service password-encryption Switch(config)# crypto key generate rsa usage-keys label sshkeys modulus 768 Switch(config)# aaa new-model Switch(config)# aaa authentication login onconsole line Switch(config)# username <switch_platform_username> secret <switch_platform_password> Switch(config)# enable secret <switch_enable_password> Switch(config)# line vty 0 15 Switch(config-line)# no password Switch(config-line)# transport input ssh Switch(config)# exit Switch(config)# line console 0 Switch(config-line)# login authentication onconsole Switch(config-line)# password <switch_console_password> Switch(config)# exit Switch(config)# ip ssh version 2 Switch(config)# no ip http server Switch(config)# no ip http secure-server Switch(config)# no ip domain lookup Switch(config)# end Switch# write memory</pre> |

Procedure 23. Cisco Switch SwitchConfig to netConfig Migration

| Step | Procedure | Results |
|--------------------------------|--|---|
| 4. <input type="checkbox"/> | Switch CLI: Reload the switch and verify configuration | If a command was not applied, repeat. <code>Switch# reload</code> If prompted, answer Yes . |
| 5. <input type="checkbox"/> | Virtual PMAC: Verify netConfig connectivity | Verify that netConfig can communicate with the switch. <code>\$ sudo /usr/TKLC/plat/bin/netConfig getHostname -- device=<switch_name></code> Hostname: <switch_name> |
| 6. <input type="checkbox"/> | Virtual PMAC: Back up the switch configuration | Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig). |
| 7. <input type="checkbox"/> | Virtual PMAC: Reset switch to factory defaults | For the 4948 series switches: <code>sudo /usr/TKLC/plat/bin/netConfig setFactoryDefault -- device=<switch_name></code> For the 3020 series switches, perform 3.3.1 Configure Cisco 3020 Switch (netConfig), steps 3. through 9. and 12. , replacing the values for the switch being replaced. |
| 8. <input type="checkbox"/> | Virtual PMAC: Restore configuration | For the 4948 series switches, perform 3.2.4 Replace a Failed 4948/4948E/4948E-F Switch (PMAC Installed) (netConfig), steps 6. through 20. For the 3020 series switches, perform 3.3.2 Replace a Failed 3020 Switch (netConfig), steps 5. through 10. |
| 9. <input type="checkbox"/> | Virtual PMAC: Repeat | Repeat steps 2. through 8. for each switch being migrated. |

3.4.9 HP 6120XG SwitchConfig to netConfig Migration

This procedure configures 6120XG switch to migrate from switchconfig to netConfig.

Needed Material

- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- Application-specific documentation (document that referred to this procedure)
- Template xml files in an application ISO on the application media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 24. HP 6120XG SwitchConfig to netConfig Migration

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Management Server: Verify network connectivity to the 6120XG switch | <pre>\$ /bin/ping -w3 <enclosure_switch_IP></pre> |
| 2. <input type="checkbox"/> | Management Server: Login | Log into the 6120XG switch using SSH or Telnet. <pre>\$ /usr/bin/ssh manager@<enclosure_switch_IP></pre> If the above command fails, log in using telnet: <pre>\$ /usr/bin/telnet <enclosure_switch_IP></pre> |
| 3. <input type="checkbox"/> | Switch CLI: Apply netConfig commands | From the 6120XG switch CLI, apply the following commands required by netConfig: <pre>Switch# config Switch(config)# hostname <switch_name> Switch(config)# no password all Password protection for all will be deleted, continue [y/n]? y Switch(config)# include-credentials</pre> Note: If prompted after include-credentials , answer Yes to both questions. <pre>Switch(config)# password manager user-name <platform_username> plaintext <platform_enable_password> Switch(config)# console flow-control none Switch(config)# ip ssh listen oobm Switch(config)# ip ssh filetransfer Switch(config)# no tftp client Switch(config)# no tftp server Switch(config)# no telnet-server Switch(config)# end Switch# write memory</pre> |
| 4. <input type="checkbox"/> | Management Server: Reload the switch and verify configuration | If a command was not applied, repeat. <pre>Switch# reload</pre> If prompted, answer Yes . |
| 5. <input type="checkbox"/> | Management Server: Verify netConfig connectivity | Verify that netConfig can communicate with the switch. <pre>\$ sudo /usr/TKLC/plat/bin/netConfig getFirmware -- device=<switch_name> Version: Z.14.32 Image: Secondary</pre> |
| 6. <input type="checkbox"/> | Management Server: Back up the switch configuration | Perform 3.2.7 Back Up Cisco 4948/4948E/4948E-F Aggregation Switch and/or Cisco 3020 Enclosure Switch (netConfig). |

Procedure 24. HP 6120XG SwitchConfig to netConfig Migration

| Step | Procedure | Results |
|--------------------------------|--|---|
| 7. <input type="checkbox"/> | Management Server: Restore configuration | Perform 3.2.4 Replace a Failed 4948/4948E/4948E-F Switch (PMAC Installed) (netConfig), steps 3. through 8. |
| 8. <input type="checkbox"/> | Management Server: Verify configuration | Once each HP 6120XG has finished booting from the previous step, verify network reachability and configuration. <pre> [admusr@localhost ~]\$ /bin/ping -w3 <enclosure_switch_IP> [admusr@localhost ~]\$ /usr/bin/ssh <switch_platform_username>@<enclosure_switch_IP> Switch# show run </pre> Inspect the output of show run, and ensure that it is configured as per site requirements. |

3.4.10 Configure DSCP Marking Using iptablesADM

This procedure configures DSCP marking using iptablesADM.

Note: DSCP marking set using the QOS procedure Configure QoS (DSCP and/or CoS) on HP 6120XG Switches may conflict/overwrite marking set using the steps below.

iptablesAdm uses a native iptables command with additional TPD driven arguments.

Generic command for DSCP marking:

```

$ sudo /usr/TKLC/plat/bin /iptablesAdm insert --table=mangle --type=rule --
protocol=[ipv4|ipv6] --domain=<domain> --chain=<chain> --match='-p [tcp|udp|icmp] -
j DSCP --set-dscp [DSCP value]' --location=<number> --persist=yes

```

Where

<table> - For DSCP marking, the table is always = mangle

<domain> - User initiated name for a set of iptables rules. Valid names start with a two-digit number and then an alphanumeric value; such as 25example.

Note: The domain sets the order of operation.

<match> - This is the native iptables command string.

<chain> - Native iptables set of rules. For the mangle table valid values are: PREROUTING, OUTPUT, FORWARD, INPUT, and POSTROUTING.

Example 1

Use this command to mark a locally generated outgoing icmp packet with the value of 18:

```

$ sudo /usr/TKLC/plat/bin/iptablesAdm insert --table=mangle --type=rule --
protocol=ipv4 --domain=<domain> --chain=POSTROUTING --match='-p icmp -j DSCP --set-
dscp 18' --location=1 --persist=yes

```

- If no domain has been previously set up this command creates the domain.
- If **persist=yes** then the rule is placed in /etc/sysconfig/iptables or /etc/sysconfig/ip6tables

The resulting user defined rule can be viewed with the command:

```

$ sudo /usr/TKLC/plat/bin/iptablesAdm show --type=rule --protocol=ipv4 --
table=mangle

```

The resulting user defined rule can be removed with the command:

```
$ sudo /sbin/iptablesAdm delete --table=mangle --type=rule --protocol=ipv4 --
domain=<domain> --chain=POSTROUTING --match='-p icmp -j DSCP --set-dscp 18'
```

Note: Either the `--match'`<native iptables command string>' or the `--location=<number>` can be used to delete a rule.

Example 2

Use this command to mark an outgoing packet leaving using the ssh port with the DSCP value 12:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm insert --table=mangle --type=rule --
protocol=ipv4 --domain=<domain> --chain=POSTROUTING --match='-p tcp --sport 22 -j
DSCP --set-dscp 12' --location=1 --persist=yes
```

The resulting user defined rule can be viewed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm show --type=rule --protocol=ipv4 --
table=mangle
```

The resulting user defined rule can be removed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --table=mangle --type=rule --
protocol=ipv4 --domain=<domain> --chain=POSTROUTING --match='-p tcp --sport 22 -j
DSCP --set-dscp 12' --location=1 --persist=yes
```

Example 3

Use this command to mark all outbound traffic on the bond1 interface with a DSCP value of 25:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm insert --type=rule --protocol=ipv4 --
domain=<domain> --chain=OUTPUT --table=mangle --match='-o bond1 -j DSCP -setdscp
25' --location=1 --persist=yes
```

The resulting user defined rule can be viewed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm show --type=rule --protocol=ipv4 --
table=mangle
```

The resulting user defined rule can be removed with the command:

```
$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --type=rule --protocol=ipv4 --
domain=<domain> --chain=OUTPUT --table=mangle --match='-o bond1 -j DSCP -setdscp
25'
```

3.4.11 Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig)

This procedure is intended only for use with 1GE LAG uplinks from HP 6125XLG enclosure switches to Cisco 4948/E/-F product aggregation switches or the customer network. Configuring speed and duplex on the LAG ports turns off autonegotiation for the individual links, and must be performed on both switches for all participating LAG links. This procedure addresses a known weakness with autonegotiation on 1GE SFPs and the 6125XLG that causes 1GE links to take longer than expected to become active.

Prerequisites:

- 3.1 Configure netConfig Repository
- 3.3.5 Configure HP 6125XLG Switch (netConfig)

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 25. Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig)

| Step | Procedure | Results |
|--|----------------------------|---|
| <p>1. <input type="checkbox"/></p> | <p>Virtual PMAC</p> | <p>List configured link aggregation groups on the 6125XLG enclosure switch. Capture the LAG id connected to the 4948/E/E-F product aggregation switch or the customer network. In the following example, LAG id 1 is identified as the 4x1GE LAG requiring speed and duplex configuration.</p> <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> getLinkAggregation Interface: LAG1: Active Link State: Up Mode: Active</pre> |
| <p>2. <input type="checkbox"/></p> | <p>Virtual PMAC</p> | <p>Get the list of interfaces configured for the LAG on the 6125XLG. In the following example, LAG id 1 is inspected, and is shown to include interfaces tenGE17-20.</p> <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> getLinkAggregation id=1 Interface: LAG1: Active Link State: Up Description: ISL to P3-Switch2 LAG Interfaces: tenGE17: Bundled tenGE18: Bundled tenGE19: Bundled tenGE20: Bundled Link State: Up Mode: Active MTU: 10000 Type: trunk Untagged Vlan: 1 Vlan Membership: 1-4094</pre> |
| <p>3. <input type="checkbox"/></p> | <p>Virtual PMAC</p> | <p>Inspect the switch LAG port configurations and verify speed and duplex are set on the LAG interfaces, as shown in this example:</p> <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> setSwitchport interface=tenGE17-20 speed=1000 duplex=full</pre> |

Procedure 25. Configure Speed and Duplex for 6125 XLG LAG Ports (netConfig)

| Step | Procedure | Results |
|--------------------------------|---------------------|---|
| 4. <input type="checkbox"/> | Virtual PMAC | Inspect the switch LAG port configurations and verify speed and duplex are set on the LAG interfaces, as shown in this example: <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> getSwitchport interface=tenGE17-20 Interface: tenGE1: Active Link State: Up Description: Ten-GigabitEthernet1/1/5 Interface Duplex: full Link State: Up Media Type: N/A MTU: Unknown Speed: 1000 Type: trunk Untagged VLAN: 1 VLAN Membership: 1-4094</pre> |

3.4.12 Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

This procedure is intended only for use with 1GE LAG uplinks from HP 6125XLG enclosure switches to Cisco 4948/E/-F product aggregation switches or the customer network. Configuring speed and duplex on the LAG ports turns off autonegotiation for the individual links, and must be performed on both switches for all participating LAG links. This procedure addresses a known weakness with autonegotiation on 1GE SFPs and the 6125XLG that causes 1GE links to take longer than expected to become active.

Prerequisites:

- 3.1 Configure netConfig Repository
- 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig)
- 3.3.5 Configure HP 6125XLG Switch (netConfig)

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 26. Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

| Step | Procedure | Results |
|-----------------|----------------------------|--|
| <p>1. □</p> | <p>Virtual PMAC</p> | <p>List configured link aggregation groups on the Cisco 4948/E/E-F. Identify the LAG(s) connected to a 6125XLG enclosure switch. In this example, the switch has 8 link aggregation groups configured, but LAG ID 2 is identified to be connected to a 6125XLG by 4x1GE LAG uplink.</p> <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> getLinkAggregation Interface: LAG1: Active Link State: Up Mode: Active LAG2: Active Link State: Up Mode: Active LAG3: Active Link State: Up Mode: Active LAG4: Active Link State: Up Mode: Active LAG5: Active Link State: Up Mode: Active LAG6: Active Link State: Up Mode: Active LAG7: Active Link State: Up Mode: Active LAG8: Active Link State: Up Mode: Active</pre> |

Procedure 26. Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

| Step | Procedure | Results |
|-----------------|----------------------------|--|
| <p>2. □</p> | <p>Virtual PMAC</p> | <p>Get the list of interfaces configured for the LAG. In the following example, LAG id 2 is inspected, and is shown to include interfaces GE9-12.</p> <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> getLinkAggregation id=2 Interface: LAG2: Active Link State: Up Description: ISL to cxeny(en2)-sw2 LAG Interfaces: GE9: Bundled GE10: Bundled GE11: Bundled GE12: Bundled Link State: Up Mode: Active MTU: 10000 Type: trunk Untagged Vlan: 1 Vlan Membership: 1-6</pre> |
| <p>3. □</p> | <p>Virtual PMAC</p> | <p>Set the speed to 1000 and duplex to full for all LAG interfaces identified in the previous step. Speed should be set to 1000 Mbps. Duplex should be set to full. In this example, speed and duplex are configured on the interfaces highlighted by the previous step, GE9-12.</p> <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> setSwitchport interface=GE9-12 speed=1000 duplex=full</pre> |
| <p>4. □</p> | <p>Virtual PMAC</p> | <p>Inspect the switch LAG port configurations and verify speed and duplex are set as shown in this example:</p> <pre>[admusr@exapmle~]\$ sudo netConfig --device=<switch_hostname> getSwitchport interface=GE9-12 Interface: GE9: Active Link State: Up Description: ISL_to_cxeny(en2)-sw2 Duplex: full Link State: Up Media Type: N/A MTU: Unknown Speed: 1000 Type: trunk Untagged VLAN: 1 VLAN Membership: 1-6 <output for remaining interfaces removed to save space></pre> |

Procedure 26. Configure Speed and Duplex for 6125 XLG LAG Ports for Cisco 4948/4948E/4948E-F (netConfig)

| Step | Procedure | Results |
|--------------------------------|--------------------------------|---|
| 5. <input type="checkbox"/> | Virtual PMAC: Repeat | Repeat steps 2. through 4. for each LAD ID. |

4. Brocade Switch — SwitchConfig Procedures

4.1 Configure Brocade Switches

This procedure configures names, user passwords, and NTP settings for Brocade switches; and backs up the configuration to the management server hosting PMAC.

Prerequisites:

- 7.1 Configure Initial OA IP
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 27. Configure Brocade Switches

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | OA Shell: Log into the active OA | <p>Log into OA via ssh as root user.</p> <pre>login as: root ----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.00 Built: 03/19/2010 @ 14:13 OA BayNumber: 1 OA Role: Active root@10.240.17.51's password:</pre> <p>If the OA role is not Active, log into the other OA of the enclosure system.</p> |

Procedure 27. Configure Brocade Switches

| Step | Procedure | Results |
|--|---|--|
| <p>2. <input type="checkbox"/></p> | <p>OA Shell: Log into the Brocade switch console</p> | <p>Run the following command to get Brocade switches bay IDs:</p> <pre>> show interconnect list OA-001F296DB1BB> show interconnect list BayInterconnect Type Manufacturer Power Health UIDManagement IP ----- 1 Ethernet Cisco Systems, Inc. On OK Off 10.240.4.70 2 Ethernet Cisco Systems, Inc. On OK Off 10.240.4.71 3 Fibre ChannelBROCADE On OK Off 10.240.4.50 4 Fibre ChannelBROCADE On OK Off 10.240.5.51 5 [Absent] 6 [Absent] 7 [Absent] 8 [Absent] Totals: 4 interconnect modules installed, 4 powered on. # connect interconnect <bay_id_number> NOTICE: This pass-thru connection to the integrated I/O console is provided for convenience and does not supply additional access control. For security reasons, use the password features of the integrated switch. Connecting to integrated switch 4 at 9600,N81... Escape character is '<Ctrl>_' (Control + Shift + Underscore) Press [Enter] to display the switch console: Press Enter twice and login as root user. swd77 console login: root Password: Change passwords for switch default accounts now. Use Control-C to exit or press 'Enter' key to proceed. Press Enter to see the prompt.</pre> |
| <p>3. <input type="checkbox"/></p> | <p>Brocade Switch Console: Set root user password</p> | <pre>swd77:root> passwd root Changing password for root Enter new password: Re-type new password: passwd: all authentication tokens updated successfully Saving password to stable storage. Password saved to stable storage successfully.</pre> |
| <p>4. <input type="checkbox"/></p> | <p>Brocade Switch Console: Set factory user password</p> | <pre>swd77:root> passwd factory</pre> |
| <p>5. <input type="checkbox"/></p> | <p>Brocade Switch Console: Set admin user password</p> | <pre>swd77:root> passwd admin</pre> |

Procedure 27. Configure Brocade Switches

| Step | Procedure | Results |
|---------------------------------|---|--|
| 6. <input type="checkbox"/> | Brocade Switch Console: Set user password | <code>swd77:root> passwd user</code> |
| 7. <input type="checkbox"/> | Brocade Switch Console: Set switch name for the FC switch | The bay ID number is the same number as the one used in step 1. to connect: <code>swd77:root> switchName bay<bay_id_number></code> <code>Committing configuration...</code> <code>Done.</code> |
| 8. <input type="checkbox"/> | Brocade Switch Console: Set chassis name for the FC switch | Use the enclosure name used during the OA setup, prepended by alphabetical character, for example, c505_05_01. <code>swd77:root> chassisName <chassis_name></code> Note: The chassis name must begin with an alphabetical character. |
| 9. <input type="checkbox"/> | Brocade Switch Console: Set NTP server on the FC switch | <code>swd77:root> tsclockserver <NTP_server_ip></code> <code>Updating Clock Server configuration...done.</code> <code>Updated with the NTPservers</code> Make sure the change was applied. <code>swd77:root> tsclockserver</code> <code>Active NTPServer 10.250.32.10</code> <code>Configured NTPServer List 10.250.32.10</code> |
| 10. <input type="checkbox"/> | Brocade Switch Console: Back up configuration | <code>swd77:root> configUpload</code> Protocol (scp, ftp, local) [ftp]: scp Server Name or IP Address [host]: <PMAC_IP> User Name [user]: pmacadmin File Name [config.txt]: /var/TKLC/smac/backup/<chassis_switch_bay> Section (all chassis [all]): pmacadmin@<ip>'s password: configUpload complete: All config parameters are uploaded where <chassis_switch_bay> would be 500_05_01_bay3, for instance. |
| 11. <input type="checkbox"/> | Brocade Switch Console: Log out | <code>swd77:root> logout</code> Press control + shift + underscore and D to logout from the FC switch console. |
| 12. <input type="checkbox"/> | Repeat | Repeat steps 2. through 11. for the second Brocade switch. |
| 13. <input type="checkbox"/> | OA: Log out | <code>> exit</code> |

4.2 Upgrade Brocade Switch Firmware

This procedure upgrades firmware for the Brocade switches. The procedure covers either 4/24 or 8/24 Brocade switches.

Prerequisites:

- 7.1 Configure Initial OA IP

Needed Material

- HP MISC firmware ISO image
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6.x is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

4.3 Configure Zones in Brocade Switches

This optional procedure should be applied to both Brocade switches that are part of the same enclosure. Zone settings have to be the same for both switches.

This procedure is optional. Skipping this procedure allows switches to connect to all ports.

Note: This procedure should be used with requirements provided by the application. There are general guidelines typically used, but the application documentation is the authoritative source:

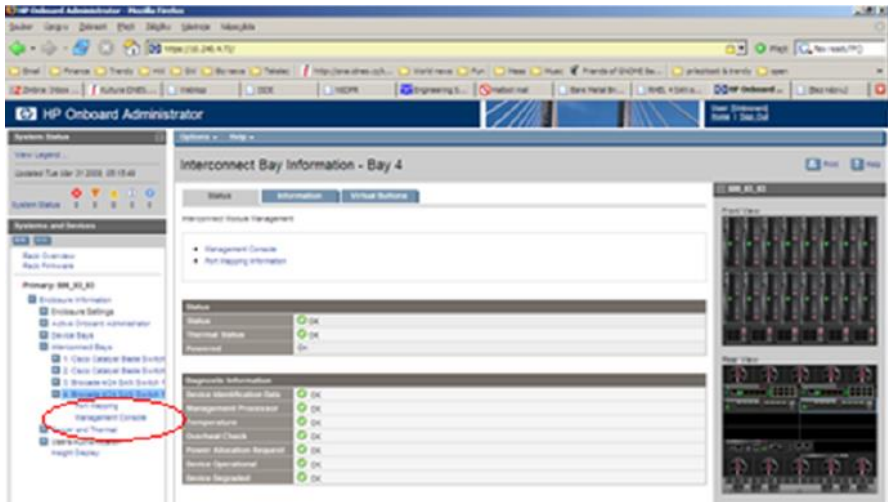
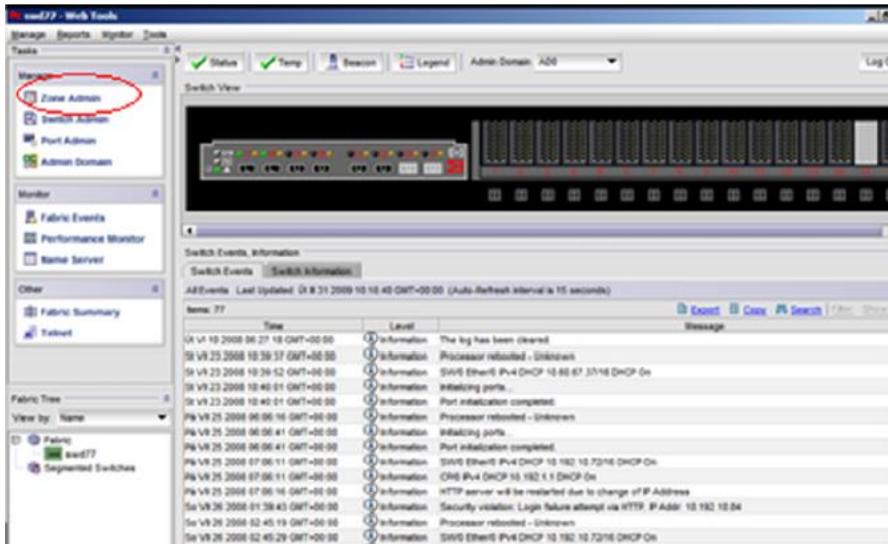
- The rules for the zone configuration: There should be one zone per one storage array in the fibre channel switch.
- Identical zones need to be created in each Brocade in the same enclosure.
- The members of such zone are all ports from the management storage array and all servers that need access to it.
- Be sure to create zones for all management storage array controllers. If a Brocade port is not in a zone, then it cannot communicate.
- After configuring specific zones, create another **catch-all** zone that covers the rest of the devices.

Prerequisites:

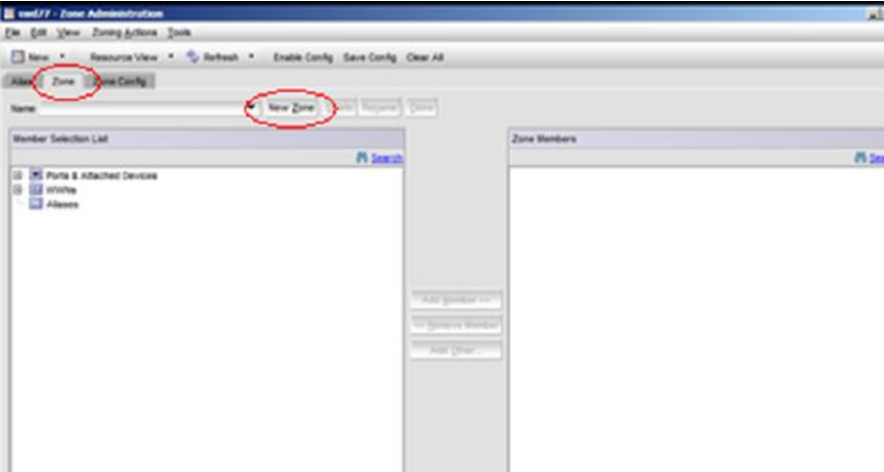
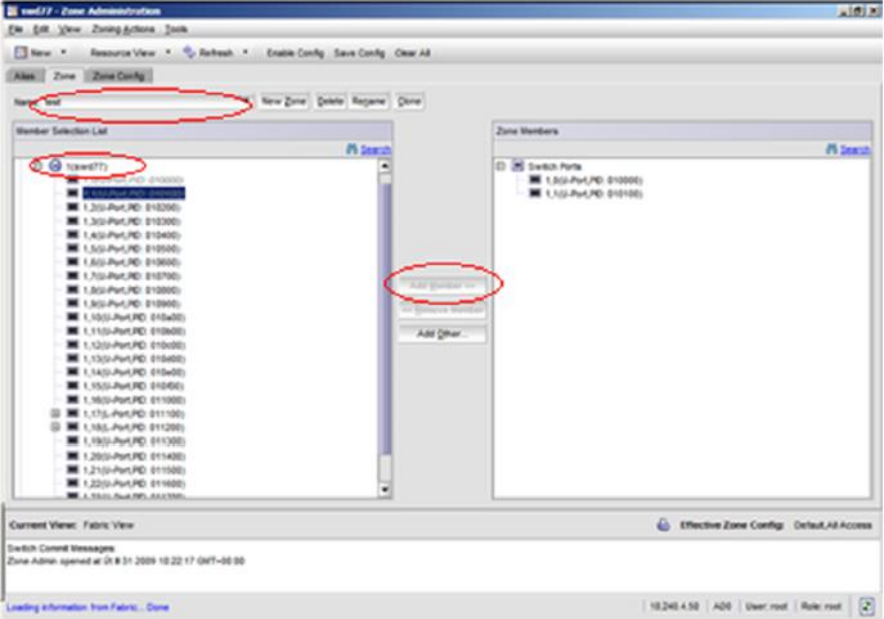
- 4.1 Configure Brocade Switches
- Know the network cabling and SAN requirements by blade server

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

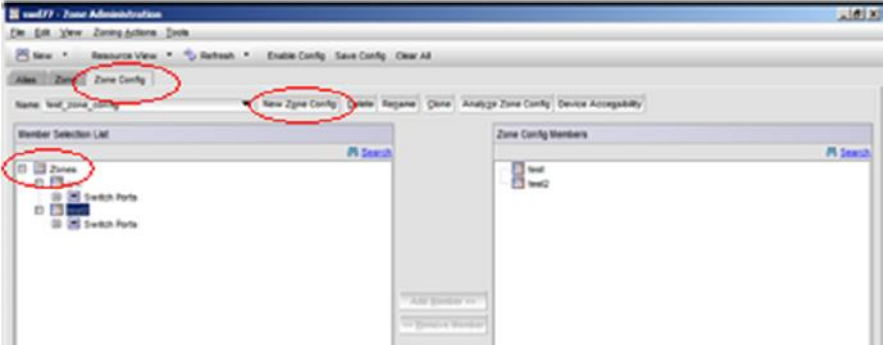
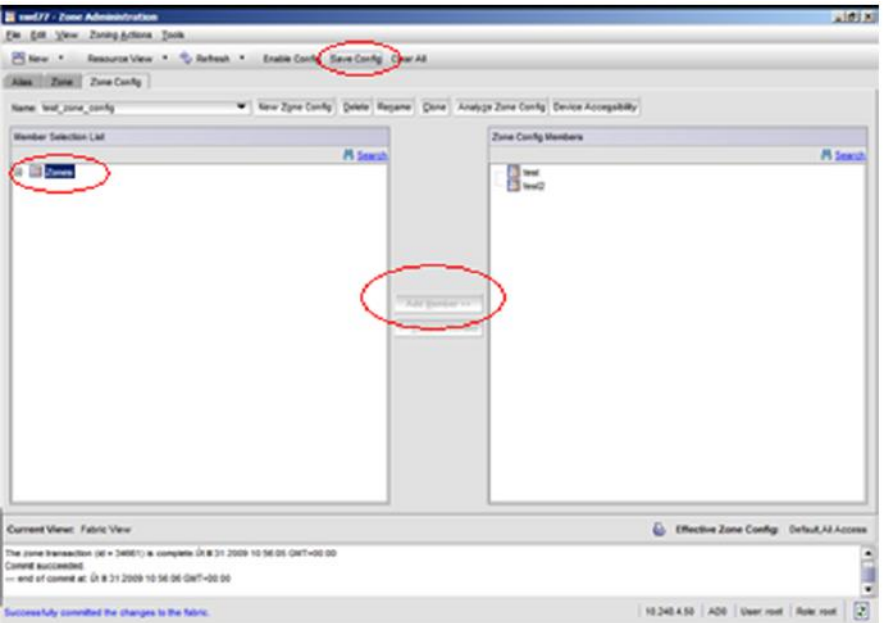
Procedure 28. Configure Zones in Brocade Switches

| Step | Procedure | Results |
|------------------------------------|---|---|
| <p>1. <input type="checkbox"/></p> | <p>OA GUI: Log into the OA and select the Fibre Channel switch</p> | <p>1. Navigate to Enclosure Information > Interconnect Bays > Brocade ... > Management Console.</p>  <p>The Fibre Channel console loads.</p> <p>2. Login as the administrative user.</p> |
| <p>2. <input type="checkbox"/></p> | <p>Fibre Channel Switch Console</p> | <p>Navigate to Zone Admin.</p>  |

Procedure 28. Configure Zones in Brocade Switches

| Step | Procedure | Results |
|---|--|---|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Fibre Channel Switch Console: Create a new zone</p> | <ol style="list-style-type: none"> Select the Zone tab.  <ol style="list-style-type: none"> Click New Zone. Type an appropriate name and click OK. |
| <p>4.</p> <p><input type="checkbox"/></p> | <p>Fibre Channel Switch Console: Add port members into the zone</p> | <ol style="list-style-type: none"> Select the zone where ports should be added. Expand the Ports and Attached Devices twice and select the ports under Ports and Attached Devices. Click Add Member.  <ol style="list-style-type: none"> Create a catch-all zone that covers all remaining devices (such as blade servers and ports) that are not in the zone specified. |

Procedure 28. Configure Zones in Brocade Switches

| Step | Procedure | Results |
|------------------------------------|---|--|
| <p>5. <input type="checkbox"/></p> | <p>Fibre Channel Switch Console: Create zone configuration</p> | <ol style="list-style-type: none"> 1. Select the Zone Config tab. 2. Click New Zone Config.  <ol style="list-style-type: none"> 3. Type an appropriate name (for example, Production_Zone_Config) and click OK. |
| <p>6. <input type="checkbox"/></p> | <p>Fibre Channel Switch Console: Add zones into zone configuration</p> | <ol style="list-style-type: none"> 1. Expand the Zones Selection List. 2. Select all desired zones and click Add Member.  <ol style="list-style-type: none"> 3. Click Save Config and Yes. 4. Observe the status at the bottom of the screen. Make sure the "Successfully committed the changes to the fabric" message displays in blue at the bottom of the screen. |

Procedure 28. Configure Zones in Brocade Switches

| Step | Procedure | Results |
|--------------------------------|---|--|
| 7. <input type="checkbox"/> | Fibre Channel Switch Console: Enable zone configuration | <ol style="list-style-type: none"> 1. Click Enable Config. 2. Select Zone Config from the option list. 3. Click OK. 4. Click Yes. 5. Observe the status at the bottom of the screen. Make sure the "Successfully committed the changes to the fabric" message displays in blue at the bottom of the screen. |
| 8. <input type="checkbox"/> | Repeat | Repeat steps 1. through 7. on second switch in the same enclosure. The two switches should have identical configurations. |

4.4 Configure Brocade Switch XNMP Trap Target

This procedure configures SNMP settings for Brocade switches.

Prerequisites:

- 4.1 Configure Brocade Switches
- Know the network cabling and SAN requirements by blade server

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 29. Configure Brocade Switch XNMP Trap Target

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | OA: Log into the Brocade switch console | <p>Log into OA via ssh as root user. Run the following command to get the Brocade switches bay IDs:</p> <pre>> show interconnect list OA-001F296DB1BB> show interconnect list Bay Interconnect Type Manufacturer Power Health UIDManagement IP ----- 1 Ethernet Cisco Systems, Inc. On OK Off 10.240.4.70 2 Ethernet Cisco Systems, Inc. On OK Off 10.240.4.71 3 Fibre Channel BROCADE On OK Off 10.240.4.50 4 Fibre Channel BROCADE On OK Off 10.240.5.51 5 [Absent] 6 [Absent] 7 [Absent] 8 [Absent] Totals: 4 interconnect modules installed, 4 powered on. Run: # connect interconnect <bay_id></pre> <p>This connects the user to the FC switch console. Press Enter twice and login as the admin user.</p> <p>Note: The switch is configured to reject SNMP sets and gets. Only the hosts listed in step 4 are able to receive traps.</p> |

Procedure 29. Configure Brocade Switch XNMP Trap Target

| Step | Procedure | Results |
|--|---|--|
| <p>2. <input type="checkbox"/></p> | <p>Brocade Switch Console: Set the SNMP parameters to the default values</p> | <pre>swd77:admin> snmpconfig --default snmpv1 ***** This command will reset the agent's SNMPv1 configuration back to factory default ***** SNMPv1 community and trap recipient configuration: Community 1: Secret C0de (rw) No trap recipient configured yet Community 2: OrigEquipMfr (rw) No trap recipient configured yet Community 3: private (rw) No trap recipient configured yet Community 4: public (ro) No trap recipient configured yet Community 5: common (ro) No trap recipient configured yet Community 6: FibreChannel (ro) No trap recipient configured yet ***** Are you sure? (yes, y, no, n): [no] yes</pre> |
| <p>3. <input type="checkbox"/></p> | <p>Brocade Switch Console: Set security level (to disable SNMP sets and gets)</p> | <pre>swd77:admin> snmpconfig --set seclevel See output. A prompt for security level displays. Select 1 and press Enter. Select SNMP GET Security Level (0 = No security, 1 = Authentication only, 2 = Authentication and Privacy, 3 = No Access): (0..3) [0] 1 Select 3 and press Enter. Select SNMP SET Security Level (0 = No security, 1 = Authentication only, 2 = Authentication and Privacy, 3 = No Access): (3..3) [3] 3 Verify settings: swd77:admin> snmpconfig --show seclevel</pre> |

Procedure 29. Configure Brocade Switch XNMP Trap Target

| Step | Procedure | Results |
|-----------------|--|---|
| <p>4. □</p> | <p>Brocade Switch Console: Set SNMP trap recipient IP addresses</p> | <pre>swd77:admin> snmpconfig --set snmpv1 SNMPcommunity and traprecipient configuration: Community (rw): [Secret Code] <new_password_rw> Trap Recipient's IP address : [0.0.0.0] Community (rw): [OrigEquipMfr] <new_password_rw> Trap Recipient's IP address : [0.0.0.0] Community (rw): [private] <new_password_rw> Trap Recipient's IP address : [0.0.0.0] Community (ro): [public] <new_password> Trap Recipient's IP address : [0.0.0.0] <trap_recipient_ip> Trap recipient Severity level : (0..5) [0] 2 Trap recipient Port : (0..65535) [162] Community (ro): [common] <new_password> Trap Recipient's IP address : [0.0.0.0] <trap_recipient_ip> Trap recipient Severity level : (0..5) [0] 2 Trap recipient Port : (0..65535) [162] Community (ro): [FibreChannel] <new_password> Trap Recipient's IP address : [0.0.0.0] Committing configuration...done.</pre> <p>Replace the passwords in the following examples with the appropriate passwords provided by the application. If only one trap recipient is required, set the IP address to 0.0.0.0.</p> <p>Verify the settings:</p> <pre>swd77:admin> snmpconfig --show snmpv1</pre> |
| <p>5. □</p> | <p>Brocade Switch Console: Set access control</p> | <p>Set access control to make sure the right hosts get access. If only one trap recipient is required, set the IP address to 0.0.0.0.</p> <pre>swd77:admin> snmpconfig --set accessControl SNMPaccess list configuration: Access host subnet area : [0.0.0.0] <trap_recipient_ip> Read/Write? (true, t, false, f): [true] f Access host subnet area : [0.0.0.0] <trap_recipient-ip> Read/Write? (true, t, false, f): [true] f Access host subnet area : [0.0.0.0] Read/Write? (true, t, false, f): [true] f Access host subnet area : [0.0.0.0] Read/Write? (true, t, false, f): [false] f Access host subnet area : [0.0.0.0] Read/Write? (true, t, false, f): [false] f Access host subnet area : [0.0.0.0] Read/Write? (true, t, false, f): [false] f Committing configuration...done.</pre> <p>Verify the settings are correct:</p> <pre>swd77:admin> snmpconfig --show accessControl</pre> |

Procedure 29. Configure Brocade Switch XNMP Trap Target

| Step | Procedure | Results |
|--------------------------------|--|--|
| 6. <input type="checkbox"/> | Brocade Switch Console: Set system location | <p>Set the system location so it is clear where the trap originates from:</p> <pre>swd77:admin> snmpconfig --set systemGroup Customizing MIB-II system variables ... At each prompt, do one of the following: o <Return> to accept current value, o enter the appropriate new value, o <Control-D> to skip the rest of configuration, or o <Control-C> to cancel any change. To correct any input mistake: <Backspace> erases the previous character, <Control-U> erases the whole line, sysDescr: [Fibre Channel Switch.] sysLocation: [End User Premise.] <e.g Cab7enclosureeliobay3> sysContact: [Field Support.] authTrapsEnabled (true, t, false, f): [true] Committing configuration...done.</pre> <p>Verify the settings are correct:</p> <pre>swd77:admin> snmpconfig --show systemGroup</pre> |
| 7. <input type="checkbox"/> | Brocade Switch Console: Log out | <pre>swd77:aadmin> logout</pre> |
| 8. <input type="checkbox"/> | Repeat | Repeats steps 1. through 7. to configure settings on the other Brocade switch in the enclosure. |

5. SAN Storage Arrays Procedures

5.1 Set IP on Fibre Channel Disk Controllers

This procedure sets the IP address for fibre channel disk controllers.

Note: Execute this procedure for only one of the two controllers.

Needed Material

- Serial access cable that ships with the given controller and laptop running Microsoft Windows with USB port.
- If setting the IP address for P2000, you may need to install the P2000 MSAUSB driver on the laptop. Use the HP Solutions Firmware Upgrade Pack ISO image and follow Appendix B Install P2000 MSA USB Driver.
- If setting the IP address for P2000, you may need [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 30. Set IP on Fibre Channel Disk Controllers

| Step | Procedure | Results |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Disk Array Serial Console: Configure IP address on Fibre Channel Disk Controller | <p>Connect to the disk array serial console with following settings:</p> <ul style="list-style-type: none"> • 115200 bps, 8 data bits, no parity, 1 stop bit, no flow control • Proprietary cable that ships with the controller is required for console access <p>You may have to login using the manage username and the corresponding password. Once at the prompt (#), execute the following commands:</p> <pre># set network-parameters ip <controller_A_IP_address> netmask <netmask> gateway <gateway_IP_address> controller a # set network-parameters ip <controller_B_IP_address> netmask <netmask> gateway <gateway_IP_address> controller b</pre> |
| 2. <input type="checkbox"/> | Disk Array Serial Console: Verify the values were entered correctly | <p>Run the following command and check the output:</p> <pre># show network-parameters</pre> <p>Since you are currently logged in at the cli, execute the following command at this time to make sure the expansion disk arrays are identified correctly:</p> <pre># rescan</pre> |

5.2 Configure Fibre Channel Disk Controllers

This procedure configures security and user settings for fibre channel disk controllers.

Prerequisite: 5.1 Set IP on Fibre Channel Disk Controllers

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 31. Configure Fibre Channel Disk Controllers

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | Fibre Channel Disk Controller: Log in | <p>Log into the fibre channel disk controller via ssh as a manage user. Output similar to the following displays:</p> <pre>login as: manage manage@10.240.5.186's password: <manage_password> HPStorageWorks MSA2012fc System Name: Platform IXP MSA2012fc System Location: 500.07 U17 Brocade Ports 17 and 18 Version: W420R45</pre> |
| 2. <input type="checkbox"/> | Fibre Channel Disk Controller: Disable http | <pre># set protocols http disabled</pre> |
| 3. <input type="checkbox"/> | Fibre Channel Disk Controller: Disable telnet | <pre># set protocols telnet disabled</pre> |

Procedure 31. Configure Fibre Channel Disk Controllers

| Step | Procedure | Results |
|--------------------------------|--|---|
| 4. <input type="checkbox"/> | Fibre Channel Disk Controller: Disable ftp | <pre># set protocols ftp disabled</pre> |
| 5. <input type="checkbox"/> | Fibre Channel Disk Controller: Delete ftp user | <pre># delete user ftp</pre> |
| 6. <input type="checkbox"/> | Fibre Channel Disk Controller: Delete admin user | This step is required if the device is a P2000 G3 array. <pre># delete user admin</pre> This account is an additional management account added by HP and is not needed. |
| 7. <input type="checkbox"/> | Fibre Channel Disk Controller: Change password for manage account | <pre># set password manage</pre> Use the appropriate password provided by the application documentation. |
| 8. <input type="checkbox"/> | Fibre Channel Disk Controller: Change password for monitor account | <pre># set password monitor</pre> Use the appropriate password provided by the application documentation. |
| 9. <input type="checkbox"/> | Fibre Channel Disk Controller: Set NTP and time zone | <pre># set controller-date <month> <day> <hh>:<mm>:<ss> <year> <time-zone> ntp enabled ntpaddress <PMAC_management_network_IP></pre> where month: jan feb mar apr may jun jul aug sep oct nov dec day: 1-31 hh: 0-23 mm: 0-59 ss: 0-59 year: four-digit number time-zone: offset from Universal Time (UT) in hours (e.g.: -7) For example: <pre># set controller-date sep 22 13:45:0 2007 -7 ntp enabled ntpaddress 69.10.36.3</pre> Check the time settings: <pre># show controller-date # show ntp-status</pre> |

Procedure 31. Configure Fibre Channel Disk Controllers

| Step | Procedure | Results |
|---------------------------------|---|--|
| 10. <input type="checkbox"/> | Fibre Channel Disk Controller: Verify settings | Verify service and security protocols status: # show protocols Verify user settings: # show users |
| 11. <input type="checkbox"/> | Fibre Channel Disk Controller: Configure SNMP trap host | # set snmp-parameters enable crit add-trap-host <target_IP> This enables delivery of critical events to the target destination. |
| 12. <input type="checkbox"/> | Fibre Channel Disk Controller: Log out | Log out from the fibre channel disk controller console. # exit |

5.3 Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

This procedure configures advanced settings on each MSA 2012fc disk controller.

Prerequisites:

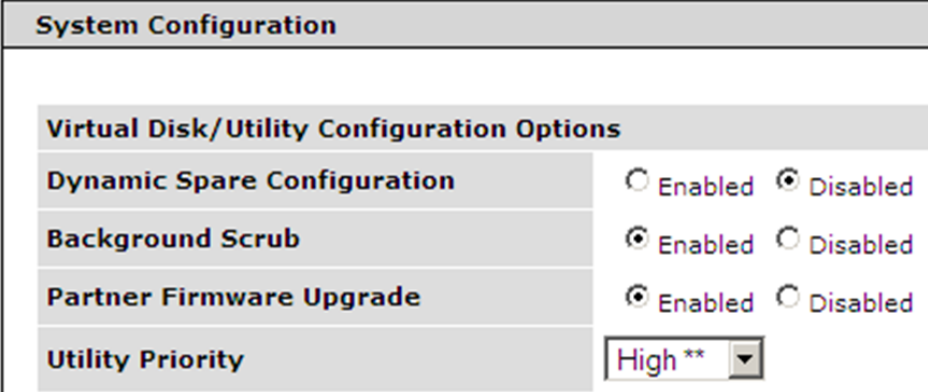
- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 32. Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Fibre Channel Disk Controller GUI: Log in | Log into the Fibre Channel Disk Controller GUI as a manage user using https: https://<fibre_channel_disk_controller_IP> |
| 2. <input type="checkbox"/> | Fibre Channel Disk Controller GUI | Navigate to Manage > General Config > System Configuration. |

Procedure 32. Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

| Step | Procedure | Results |
|--|---|---|
| <p>3. <input type="checkbox"/></p> | <p>Fibre Channel Disk Controller GUI: Change advanced settings</p> | <p>1. Make sure:</p> <ul style="list-style-type: none"> Dynamic Spare Configuration is disabled. Background Scrub is enabled. Partner Firmware Upgrade is enabled.  <p>2. Press Change System Configuration.</p> |
| <p>4. <input type="checkbox"/></p> | <p>Fibre Channel Disk Controller GUI: Verify settings</p> | <p>Verify the successful message displays.</p> |
| <p>5. <input type="checkbox"/></p> | <p>Fibre Channel Disk Controller GUI: Log out</p> | <p>Click Log Off on the left hand side.</p> |

5.4 Configure Advanced Settings on P2000 Fibre Channel Disk Controllers

This procedure configures advanced settings on each P2000 controller.

Prerequisites:

- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 33. Configure Advanced Settings on P2000 Fibre Channel Disk Controllers

| Step | Procedure | Results |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Fibre Channel Disk Controller: Login | Log into the fibre channel disk controller via ssh as a manage user. Output similar to the following displays: <pre>login as: manage manage@10.240.4.205's password: <manage_password> HPStorageWorks MSASStorage P2000G3 FC/iSCSI System Name: Uninitialized Name System Location: Uninitialized Location Version: L200R010</pre> |
| 2. <input type="checkbox"/> | Fibre Channel Disk Controller: Configure advanced settings | <pre># set advanced-settings dynamic-spare disabled Info: Command completed successfully. - Parameter 'dynamic-spare' was set to 'disabled'. Success: Command completed successfully. - The settings were changed successfully. # set advanced-settings background-scrub enabled Info: Command completed successfully. - Parameter 'background-scrub' was set to 'enabled'. Success: Command completed successfully. - The settings were changed successfully. # set advanced-settings partner-firmware-upgrade enabled Info: Command completed successfully. - Parameter 'partner-firmware-upgrade' was set to 'enabled'. Success: Command completed successfully. - The settings were changed successfully.</pre> |
| 3. <input type="checkbox"/> | Fibre Channel Disk Controller: Verify advanced setting | <pre># show advanced-settings</pre> |
| 4. <input type="checkbox"/> | Fibre Channel Disk Controller: Log out | Log out from the fibre channel disk controller console. <pre># exit</pre> |

5.5 Upgrade Firmware on MSA 2012 fc Disk Controllers

This procedure upgrades the firmware of the MSA 2012fc disk controller.

Prerequisite: 5.3 Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers

Needed Material

- HP MISC firmware ISO image
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

Note: Execute this procedure only on the A controller; the B controller automatically upgrades after the A controller.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6.x is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

5.6 Upgrade Firmware on MSA P2000 Disk Controllers

This procedure upgrades the firmware of the MSA P2000 disk controller.

Prerequisite: 5.4 Configure Advanced Settings on P2000 Fibre Channel Disk Controllers

Needed Material

- HP MISC firmware ISO image
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

Notes:

- Execute this procedure only on the A controller; the B controller automatically upgrades after the A controller.
- This procedure also upgrades any I/O modules of P2000 JBOD enclosures cascaded from the P2000 disk controller being upgraded.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6.x is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

5.7 Replace a Failed Disk in MSA 2012fc Array

The MSA 2012fc arrays should be configured with spare disks. The designation and type of spare should always be recorded for future reference.

When a disk fails, the system looks for a dedicated spare first to reconstruct the vdisk. If it does not find a properly sized dedicated spare, it looks for a global spare. A properly sized vdisk spare is one whose capacity is equal to or greater than that of the largest disk in the vdisk. A properly sized global spare is one whose capacity is equal to or greater than that of the largest disk in the disk array. Ideally, the disk that failed in the first place should still be physically replaced by a new disk and designated as the dedicated spare or a global spare, the decision depends on what kind of spare was used to reconstruct the vdisk.

If no properly sized spares are available, the vdisk reconstruction does not start automatically. To start reconstruction manually, replace each failed disk with an appropriately sized disk and add each new disk as a dedicated spare.

During the vdisk reconstruction, you can continue to use the vdisk. When a spare replaces a disk in a vdisk, the spare's icon in the enclosure view changes to match the other disks in that vdisk.

The array can indicate a failure has occurred in several ways:

- SNMP trap is sent, if controller is configured to send SNMP traps (it should be).
- Failed drive has amber LED illuminated.
- If you log into the disk controller, a screen display to indicates which disk(s) failed.

Prerequisites:

- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

Note: The vdisk reconstruction can take hours or days to complete depending on the vdisk RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop reconstruction only by deleting the vdisk.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 34. Replace a Failed Disk in MSA 2012fc Array

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Fibre Channel Disk Controller GUI: Log in | Log into the Fibre Channel Disk Controller GUI as a manage user using https: <a href="https://<fibre_channel_disk_controller_IP>">https://<fibre_channel_disk_controller_IP> |
| 2. <input type="checkbox"/> | Fibre Channel Disk Controller GUI: Clear metadata | If the replacement disk has been used in another MSA 2012fc array, it has metadata stored on it. This data must be cleared before the disk can be used in the new array. The disks, which need their metadata to be cleared, are in a Leftover or L state. 1. Navigate to Manage > Utilities > Disk Drive Utilities > Clear Metadata. 2. Select the disk(s) in an L state. 3. Click Clear Metadata for Selected Disk Drives. |
| 3. <input type="checkbox"/> | Fibre Channel Disk Controller GUI: Add global spare disk | 1. To add a global spare to reconstruct a vdisk, navigate to Manage > Virtual Disk Config. 2. Click Global Spare menu and Add Global Spares. 3. Select the disk that was replaced by marking the checkbox. It should be bright green with an A on it. 4. Click Add Global Spares toward the bottom of the screen. 5. Verify the color of the disk changes and a G displays on the disk. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen. |
| 4. <input type="checkbox"/> | Fibre Channel Disk Controller GUI: Add a dedicated spare disk | 1. To add a dedicated spare to reconstruct a vdisk, navigate to Manage > Virtual Disk Config. 2. Click vdisk configuration and Add Vdisk Spares. 3. Select the vdisk at the top of the screen. It should be bright green with an A on it. 4. Ensure the disk is in the correct enclosure and select the disk by marking the checkbox. 5. Click the Add Vdisk Spares toward the bottom of the screen. The disk changes to the same shade of blue (grey) as the rest of the disks in the enclosure. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen. 6. Log off the disk controller by clicking Log Off. |

5.8 Replace a Failed Disk in MSA P2000 Disk Array

The MSA P2000 arrays should be configured with spare disks. The designation and the type of spare should always be recorded for future reference.

When a disk fails, the system looks for a dedicated spare first to reconstruct the vdisk. If it does not find a properly sized dedicated spare, it looks for a global spare. A properly sized vdisk spare is one whose capacity is equal to or greater than that of the largest disk in the vdisk. A properly sized global spare is one whose capacity is equal to or greater than that of the largest disk in the disk array. Ideally, the disk that failed in the first place should still be physically replaced by a new disk and designated as the dedicated spare or a global spare, the decision depends on what kind of spare was used to reconstruct the vdisk.

If no properly sized spares are available, the vdisk reconstruction does not start automatically. To start reconstruction manually, replace each failed disk by appropriately sized disk and then add each new disk as a dedicated spare.

During the vdisk reconstruction, you can continue to use the vdisk. When a spare replaces a disk in a vdisk, the spare's icon in the enclosure view changes to match the other disks in that vdisk.

The array can indicate a failure has occurred in several ways:

- SNMP trap is sent, if controller is configured to send SNMP traps (it should be).
- Failed drive has amber LED illuminated.
- If you log into the disk controller, a screen display to indicates which disk(s) failed.

Prerequisites:

- 5.1 Set IP on Fibre Channel Disk Controllers
- 5.2 Configure Fibre Channel Disk Controllers

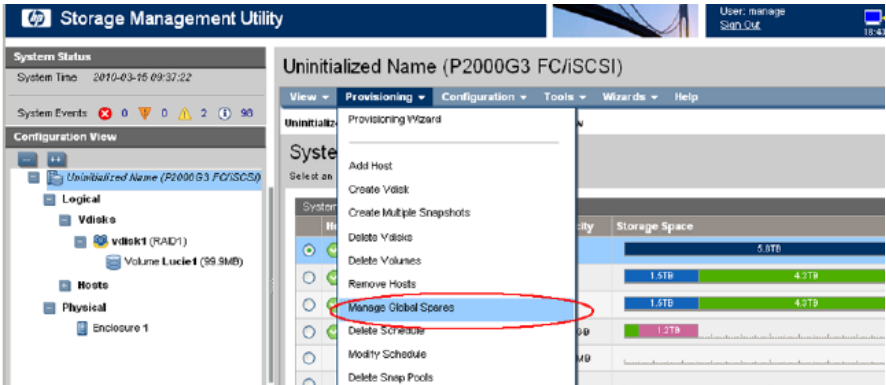

Note: The vdisk reconstruction can take hours or days to complete depending on the vdisk RAID level and size, disk speed, utility priority, and other processes running on the storage system. You can stop reconstruction only by deleting the vdisk.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

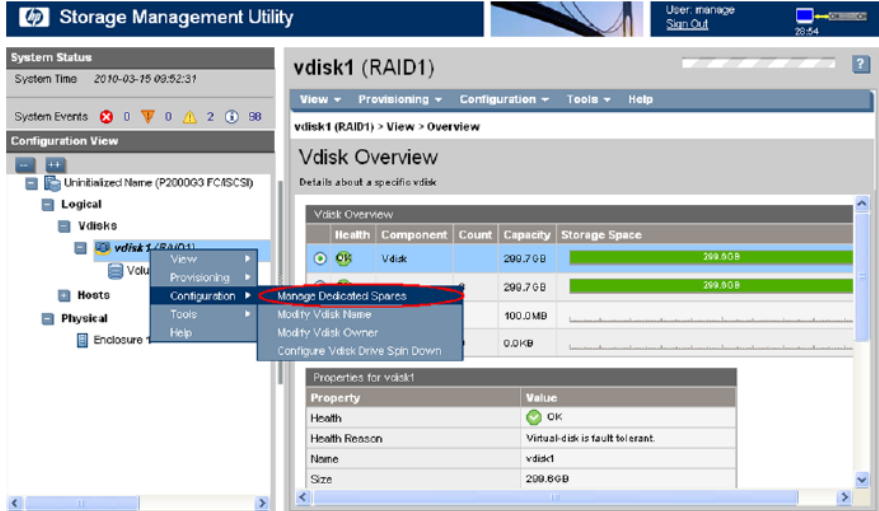

Procedure 35. Replace a Failed Disk in MSA P2000 Disk Array

| Step | Procedure | Results |
|---------|--|---|
| 1. □ | Fibre Channel Disk Controller GUI: Log in | Log into the Fibre Channel Disk Controller GUI as a manage user using https: <a href="https://<fibre_channel_disk_controller_IP>">https://<fibre_channel_disk_controller_IP> |

Procedure 35. Replace a Failed Disk in MSA P2000 Disk Array

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>2. <input type="checkbox"/></p> | <p>Fibre Channel Disk Controller GUI: Clear metadata</p> | <p>If the replacement disk has been used in another P2000 array, it has metadata stored on it. This data must be cleared before the disk can be used in the new array. The disks, which need their metadata to be cleared, are in a Leftover state.</p> <ol style="list-style-type: none"> In the Configuration View panel, right-click the system and click Tools > Clear Disk Metadata. In the main panel, select the disk(s) in an LEFTOVR state. Click Clear Metadata. <p>When processing is complete, a success screen displays.</p> <ol style="list-style-type: none"> Click OK. |
| <p>3. <input type="checkbox"/></p> | <p>Fibre Channel Disk Controller GUI: Add global spare disk</p> | <p>To add a global spare to reconstruct a vdisk, in the Configuration View panel, right-click on the system. On the right hand side blue bar menu, click Provisioning and select Manage Global Spares.</p>  <p>Switch to Graphical representation if needed. Select the disk that was replaced by marking the checkbox. It is labeled with an AVAIL on it. Click Modify Spares.</p>  <p>Verify the color of the disk changes to blue and a GLOBALSP displays on the disk. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen.</p> |

Procedure 35. Replace a Failed Disk in MSA P2000 Disk Array

| Step | Procedure | Results |
|---|---|---|
| <p>4.</p> <p><input type="checkbox"/></p> | <p>Fibre Channel Disk Controller GUI: Add a dedicated spare disk</p> | <p>To add a dedicated spare to reconstruct a vdisk, in the Configuration View panel, right-click on the vdisk and navigate to Configuration > Manage Dedicated Spares.</p>  <p>Switch to Graphical representation if needed. Ensure the disk is in the correct enclosure and select the disk by marking the checkbox. It is labelled with an AVAIL on it.</p>  <p>Click Modify Spares.</p> <p>Verify the color of the disk changes to green and SPARE displays on the disk. If there is a problem, a screen explains the failure. Popups must be allowed for this message to be seen.</p> <p>Log off the disk controller by clicking Log Off.</p> |

6. Blade Server Procedures

6.1 Upgrade Blade Server Firmware

If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP.

Note: This procedure uses a custom SPP version that cannot be obtained from the customer and, therefore, cannot be used for a Software Centric Customer. Software Centric Customers must ensure their firmware versions match those detailed in [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

This procedure upgrades the firmware on the blade servers.

The HP Support Pack for ProLiant installer automatically detects the firmware components available on the target server and only upgrades those components with firmware older than what is on the current ISO.

Prerequisite: TPD has to have been installed on the server.

Needed Material

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- USB Flash Drive (4GB or larger and formatted as FAT32) if upgrading with USB media.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6.x is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

6.2 Confirm/Upgrade Blade Server BIOS Settings

6.2.1 BIOS Settings for HP Systems

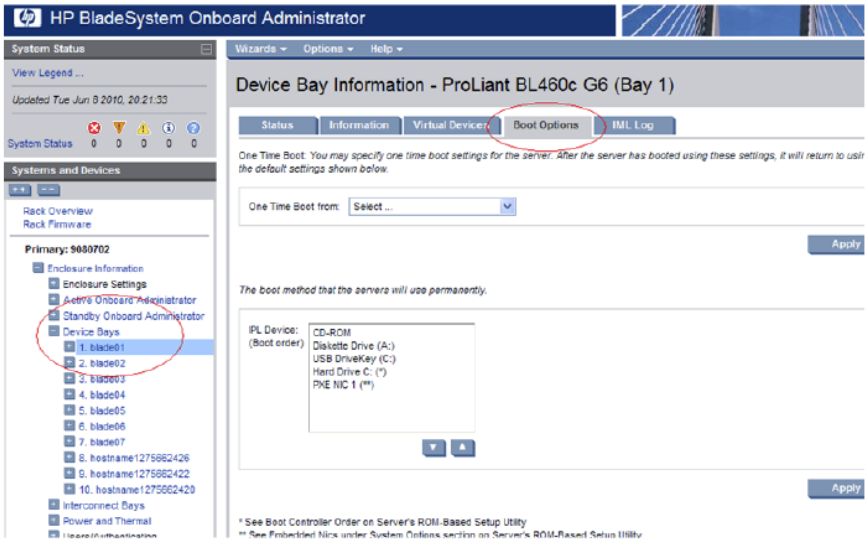
This procedure confirms and updates the BIOS boot order on the blade servers.

Prerequisite: 6.1 Upgrade Blade Server Firmware has been completed.

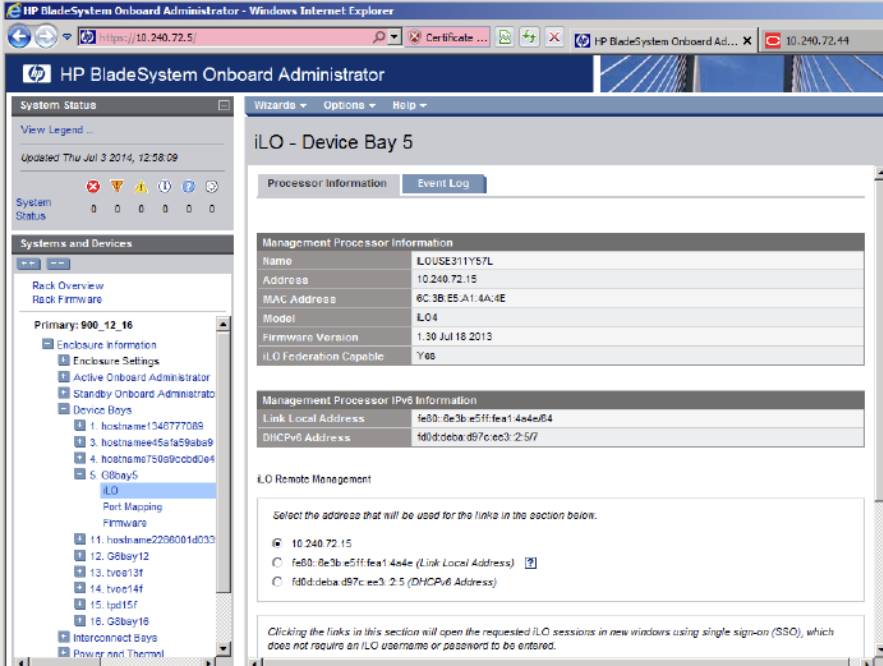
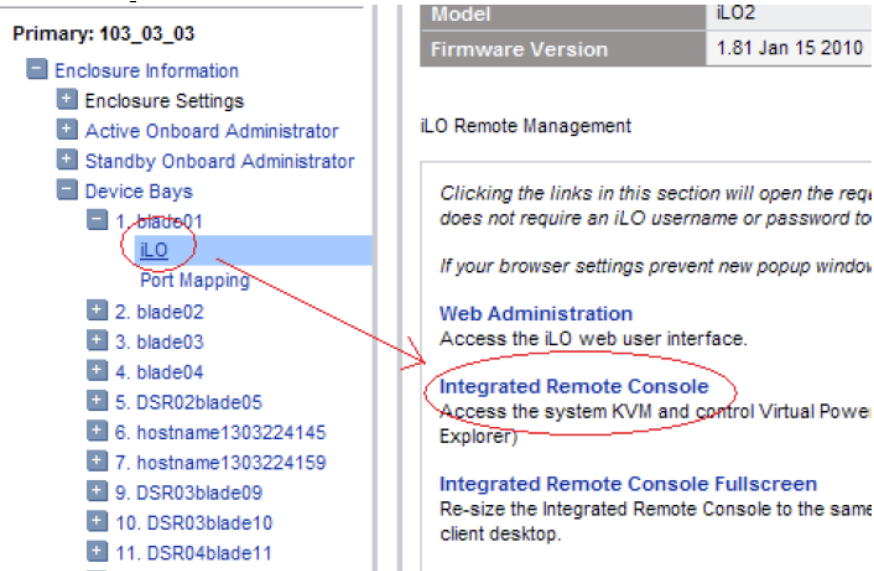
For instructions on configuring Gen9 BIOS settings, refer to [1] TPD Initial Product Manufacture Software Installation Procedure.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

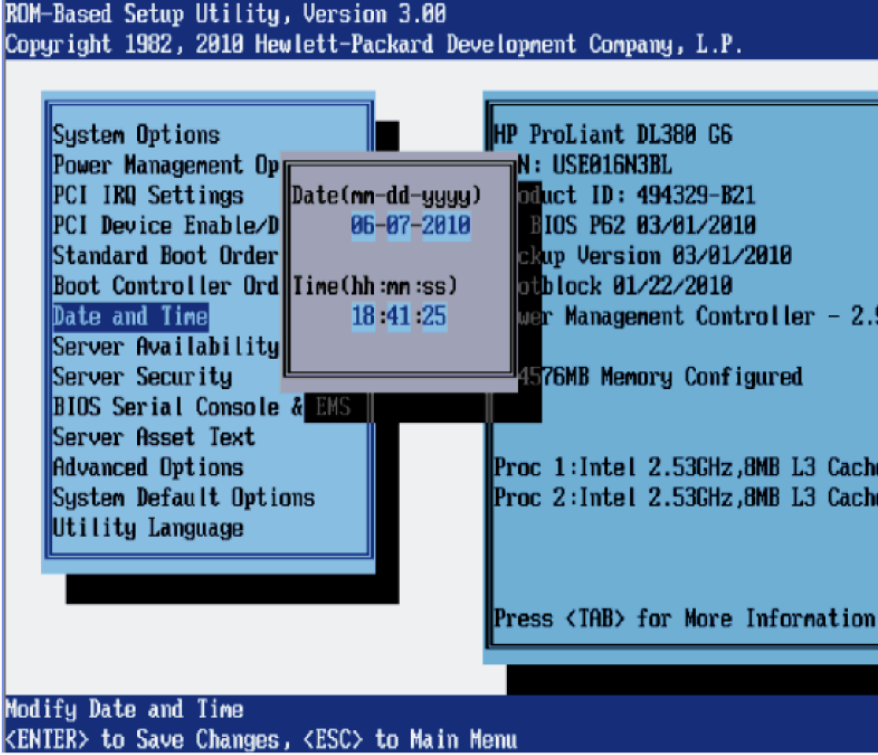
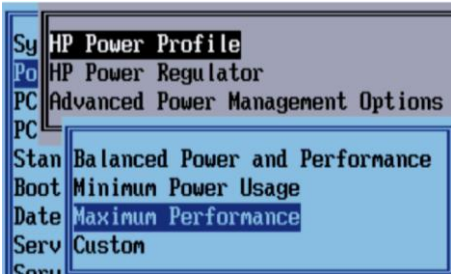
Procedure 36. BIOS Settings for HP Systems

| Step | Procedure | Results |
|---------|--|---|
| 1. □ | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |
| 2. □ | OA Web GUI: Verify boot device order | <ol style="list-style-type: none"> Navigate to Enclosure Information > Device Bays > <Blade 1>. Click on the Boot Options tab.  <ol style="list-style-type: none"> Verify the boot order is: <ul style="list-style-type: none"> CD-ROM Diskette Drive (A:) USB DriveKey (C:) Hard Drive C: (*) PXE NIC 1 (**) <p>If it is not, use the arrows to adjust the order and click Apply.</p> |

Procedure 36. BIOS Settings for HP Systems

| Step | Procedure | Results |
|---|--|--|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>OA Web GUI: Access the blade iLO</p> | <ol style="list-style-type: none"> Navigate to Enclosure Information > Device Bays > <[device]> > iLO. In iLO Remote Management, select the address. If the option to select from multiple addresses displays, select the appropriate static address.  <ol style="list-style-type: none"> Click Integrated Remote Console. This opens the iLO interface for that blade. If this is the first time the iLO is being accessed, you are asked to install and add on to your web browser. Follow the instructions to do so.  |

Procedure 36. BIOS Settings for HP Systems

| Step | Procedure | Results |
|---|--|--|
| <p>4.</p> <p><input type="checkbox"/></p> | <p>Server iLO: Update BIOS settings</p> | <ol style="list-style-type: none"> If a certificate security warning displays, click continue. Log into the blade as the admusr. Reboot the server and press F9 during the power-up sequence to access the BIOS setup screen. Navigate to Date and Time and press Enter. Set the current date and UTC time, and press Enter.  <ol style="list-style-type: none"> Press Esc to go back to the main menu. Navigate to Power Management Options and press Enter. Select the HP Power Profile and press Enter. Navigate to Maximum Performance and press Enter.  <ol style="list-style-type: none"> Press Esc twice to exit the BIOS setup screen and F10 to confirm exiting the utility. <p>The blade reboots.</p> |

Procedure 36. BIOS Settings for HP Systems

| Step | Procedure | Results |
|--------------------------------|------------------------------|---|
| 5. <input type="checkbox"/> | OA Web GUI: Repeat | Repeat steps 2. through 4. for remaining blades and then exit the OA GUI. |

6.2.2 BIOS Settings for Oracle Sun Systems

This procedure configures the BIOS power management and UEFI settings.

For all TPD supported Oracle servers, the Energy Performance should be set to **Performance**, and on the Oracle X4-2 servers, you must set UEFI Configuration Synchronization so that **Synchronization Late** is Disabled. If this step is not performed, the server may reboot a second time after POST on some reboots. This can be especially bothersome when trying to do a one-time boot to USB or CD/DVDROM.

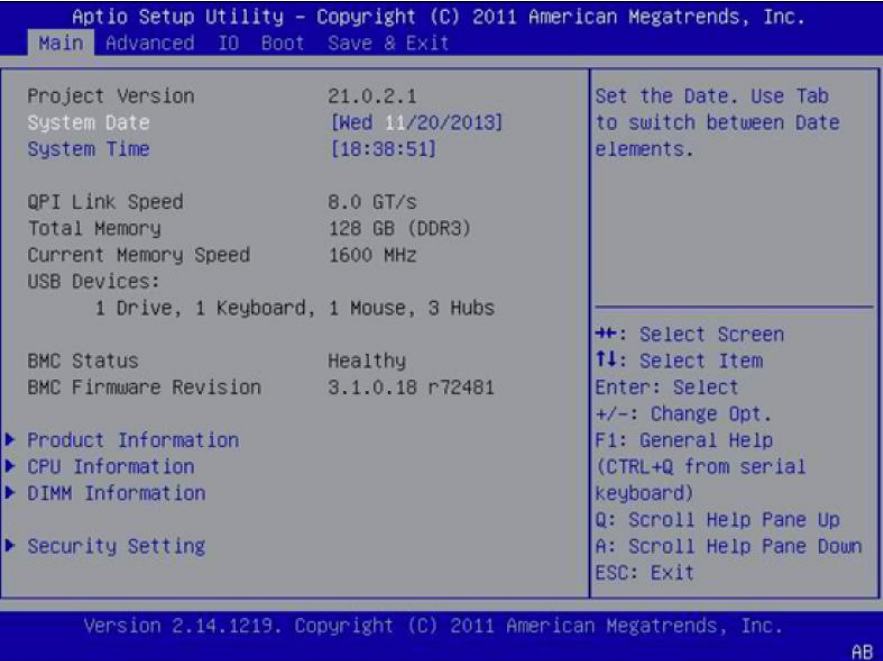
Note: In the following steps, unless stated otherwise, **X5-2**, **X6-2**, and **X7-2** refer to all versions of the X5-2, X6-2, X7-2 servers supported by TPD. For example, the Netra X5-2 server, Oracle X5-2 server, and Oracle X5-2M server apply for all mentions of X5-2.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

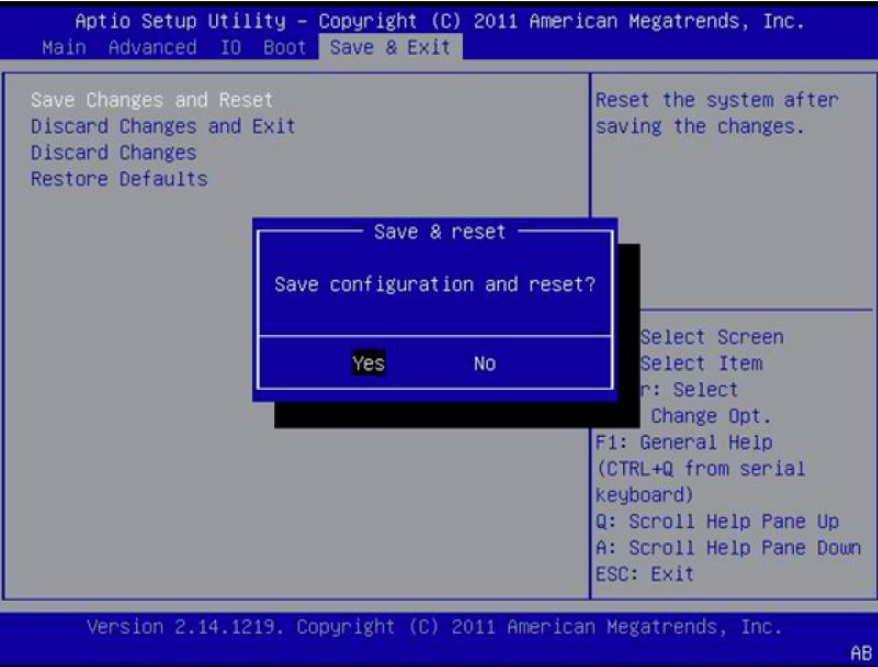
Procedure 37. BIOS Settings for Oracle Sun Systems

| Step | Procedure | Results |
|--------------------------------|------------------------------|--|
| 1. <input type="checkbox"/> | Oracle ILOM: Login | Connect to the ILOM as described in and Appendix E.1 Access a Server Console Remotely login. |

Procedure 37. BIOS Settings for Oracle Sun Systems

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>2. <input type="checkbox"/></p> | <p>Oracle ILOM: Update BIOS settings</p> | <ol style="list-style-type: none"> 1. Reboot the server and press F2 during the power-up sequence to access the BIOS setup screen. 2. Set the current date and UTC time.  <ol style="list-style-type: none"> 3. For X4-2, from the Advanced tab, select Processors. <ul style="list-style-type: none"> Note: If the server is an X5-2, X6-2, or X7-2, skip this step and go to the next step. 4. Select CPU Power Management Configuration. 5. If the Energy Performance field is not set to Performance, select Energy Performance and press Enter. <ul style="list-style-type: none"> Note: For X5-2 and X6-2, set ENERGY_PERF_BIAS_CFG mode to PERF. Press Enter and skip to step 7. 6. Select the Performance option and press Enter. 7. Press Esc twice (just once on the X5-2 and X6-2) to return to the Advanced menu. |
| <p>3. <input type="checkbox"/></p> | <p>Oracle ILOM: Update BIOS setting for the X4-2 only</p> | <ol style="list-style-type: none"> 1. Select UEFI Configuration Synchronization and press Enter. 2. If Synchronization Late is not Disable, press Enter to modify the option. Select Disabled and press Enter. 3. Press Esc to return to the Advanced menu. |

Procedure 37. BIOS Settings for Oracle Sun Systems

| Step | Procedure | Results |
|-----------------|---------------------------------|--|
| <p>4. □</p> | <p>Oracle ILOM: Boot</p> | <ol style="list-style-type: none"> Navigate to the Boot tab. For X4-2, X5-2, and X6-2, under Legacy Boot Option Priority, verify the RAID Adapter is listed first. If not, highlight it and press the + key to move it to the top of the list. For X7-2, under UEFI Boot Option Priority, verify the TPD XX.XX is listed first. If not, highlight it and press Enter to move it to Boot Option #1. Select Exit or from the Save & Exit tab, and select Save Changes and Exit. Answer Yes when asked to confirm.  |

6.3 Configure Blade Server iLO Password for Administrator Account

This procedure changes the blade server iLO password for the Administrator account for blade servers in an enclosure.

Prerequisites:

- 7.1 Configure Initial OA IP
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 38. Configure Blade Server iLO Password for Administrator Account

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | PMAC: Login | SSH into the PMAC and login as admusr . <pre>login as: admusr Password: <admusr_password></pre> |
| 2. <input type="checkbox"/> | PMAC: Create XML file | 1. In /usr/TKLC/smac/html/public-configs create an xml file with information similar to the following example. Change the Administrator password field only as instructed by the application. Note: If using a text editor like VIM, take care to use sudo before the command; otherwise, you may not be able to save the file. <pre><RIBCL VERSION="2.0"> <LOGIN USER_LOGIN="admusr" PASSWORD="password"> <USER_INFO MODE="write"> <MOD_USER USER_LOGIN="Administrator"> <PASSWORD value="<new Administrator password>" /> </MOD_USER> </USER_INFO> </LOGIN> </RIBCL></pre> 2. Save this file as change_ilo_admin_passwd.xml . 3. Change the permission of the file. <pre>\$ sudo chmod 644 change_ilo_admin_passwd.xml</pre> |
| 3. <input type="checkbox"/> | OA Shell: Log into the active OA | Log into OA via ssh as root user. <pre>login as: root</pre> <pre>----- WARNING: This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law. ----- Firmware Version: 3.00 Built: 03/19/2010 @ 14:13 OA BayNumber: 1 OA Role: Active root@10.240.17.51's password:</pre> If the OA role is not Active , log into the other OA of the enclosure system. |
| 4. <input type="checkbox"/> | OA Shell: Run hponcfg | <pre>> hponcfg all https://<pmac_ip>/public- configs/change_ilo_admin_passwd.xml</pre> |
| 5. <input type="checkbox"/> | OA Shell: Check output | Monitor the output for error messages. Refer to the HP <i>Integrate Lights-Out Management processor Scripting and Command Line Resource Guide</i> for troubleshooting. |
| 6. <input type="checkbox"/> | OA Shell: Log out | Log out from the OA. |

Procedure 38. Configure Blade Server iLO Password for Administrator Account

| Step | Procedure | Results |
|--------------------------------|---------------------------------------|--|
| 7. <input type="checkbox"/> | PMAC: Remove temporary file | On the PMAC, remove the configuration file you created. This is done for security reasons, so that no one can reuse the file: <pre>\$ sudo /bin/rm -rf /usr/TKLC/smac/html/public-configs/change_ilo_admin_passwd.xml</pre> |

6.4 Access the Server Virtual Serial Port

This procedure accesses iLO or ILOM VSP.

Prerequisite: For HP servers, complete 6.3 Configure Blade Server iLO Password for Administrator Account.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 39. Access the Server Virtual Serial Port

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | For HP Servers HP iLO: Access VSP | Login via ssh to the iLO IP as the Administrator user. <pre># ssh Administrator@<ilo_ip> Administrator@<ilo_ip>'s password: User:Administrator logged-in to ILOUSE8068S2T.nc.tekelec.com(10.250.36.71) iLO Advanced 1.50 at 17:30:27 INT=4Mar 12 2008 Server Name: localhost.localdomain Server Power: On </>hpiLO-> vsp Starting virtual serial port Press 'ESC (' to return to the CLI Session </>hpiLO-> Virtual Serial Port active: IO=0x03F8</pre> <p>Press Enter + (to refresh the screen. Note: Press ESC to escape VSP console.</p> |
| 2. <input type="checkbox"/> | For Oracle Servers Oracle ILOM: Login and connect | Login via ssh as the root user. <pre># ssh root@<ilom_ip> Password: Oracle(R) Integrated Lights Out Manager Version 3.1.0.18 r72481 Copyright (c) 2012, Oracle and/or its affiliates. All rights reserved. Warning: password is set to factory default -> start /HOST/console/ Are you sure you want to start /HOST/console (y/n)? y Serial console started. To stop, type ESC (</pre> <p>Press Enter + (to refresh the screen. Note: Press ESC to escape VSP console.</p> |

6.5 Configure Syscheck Default Route Ping Test

This procedure configures a ping test on the blade system.

Prerequisite: TPD must be installed on the blade server.

Note: Repeat this test for every blade server in the blade system.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 40. Configure Syscheck Default Route Ping Test

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Blade Server: Configure syscheck default route test | <ol style="list-style-type: none"> Log into the blade server as admusr. Enable syscheck default router test. <pre>\$ sudo /usr/TKLC/plat/bin/syscheckAdm net defaultroute -enable</pre> Run syscheck to verify the test is working. <pre>\$ sudo /usr/TKLC/plat/bin/syscheck -v net defaultroute</pre> Running modules in class net... OK LOG LOCATION: /var/TKLC/log/ syscheck/fail_log Restart syscheck. <pre>\$ sudo /sbin/initctl/syscheck restart</pre> Repeat for each blade server. |

6.6 Prepare a System for Extended Power Outage

This procedure shuts down a system properly for an extended period such as shipping from one site to another site.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 41. Prepare a System for Extended Power Outage

| Step | Results |
|--------------------------------|---|
| 1. <input type="checkbox"/> | Refer to instructions provided by the application to correctly power down all blade servers. |
| 2. <input type="checkbox"/> | Verify each server has shut down. |
| 3. <input type="checkbox"/> | Login via SSH into one fibre channel controller in each MSA as the manage user and run: <pre># shutdown both</pre> |
| 4. <input type="checkbox"/> | Power down disk arrays using power switches on each array. |
| 5. <input type="checkbox"/> | Login to each management server via SSH as admusr and run: <pre>\$ sudo /sbin/shutdown -h now</pre> |

Procedure 41. Prepare a System for Extended Power Outage

| Step | Results |
|--------------------------------|--|
| 6. <input type="checkbox"/> | If the aggregation switches are provided by Oracle, power off the 4948/4948E switches. If the aggregation switches are provided by the customer, request the customer follow their policies for preparing devices for an extended power outage. |

6.7 Bring Up a System After Extended Power Outage

This procedure powers up the HP blade system properly.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 42. Bring Up a System After Extended Power Outage

| Step | Results |
|--------------------------------|--|
| 1. <input type="checkbox"/> | Power on the cabinets that house the devices. |
| 2. <input type="checkbox"/> | If the aggregation switches are provided by Oracle, power on the 4948/4948E switches. |
| 3. <input type="checkbox"/> | Turn on the management server by depressing the power button on the front of the server. |
| 4. <input type="checkbox"/> | Turn on power switches on all disk arrays. |
| 5. <input type="checkbox"/> | Power on remaining cabinets. Ensure all power supply LEDs are green on all equipment. |
| 6. <input type="checkbox"/> | Power up each blade server. |

7. C7000 Enclosure Procedures

7.1 Configure Initial OA IP

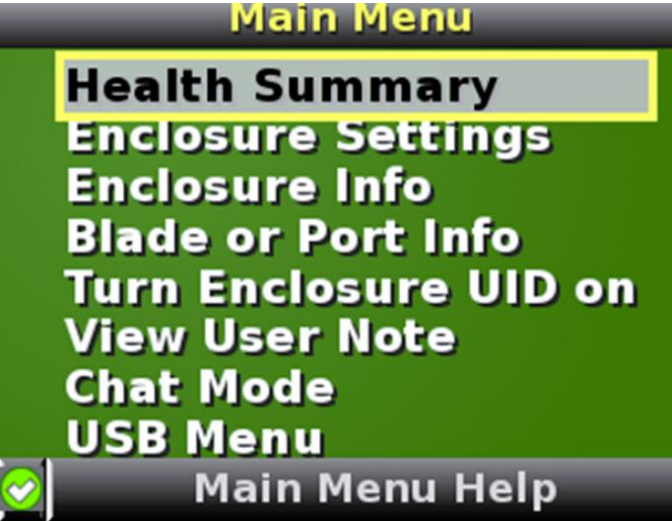

This procedure sets the initial IP address for the onboard administrator in location OA Bay 1 (left as viewed from the rear) and Bay 2 using the front panel display.

Prerequisite: Onboard administrator must be preset in the OA Bay 1 location.

Note: The enclosure should be provisioned with two onboard administrators. This procedure needs to be executed only for OA Bay 1 regardless of the number of OAs installed in the enclosure.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 43. Configure Initial OA IP

| Step | Procedure | Results |
|-----------------|-----------|---|
| <p>1. □</p> | | <p>Configure OA Bay1 IP address using insight display on the front side of the enclosure.</p>  |
| <p>2. □</p> | | <p>1. Navigate to Enclosure Settings and click OK.</p>  <p>Note: The OA1 IP and OA2 IP menu settings in this procedure may indicate OA1 IPv4 or OA1 IPv6. In either case, select this menu setting to set the OA IP address.</p> <p>2. Navigate to the OA1 IP menu settings and click OK.</p> |

Procedure 43. Configure Initial OA IP

| Step | Procedure | Results |
|--|---------------------------|---|
| <p>3. <input type="checkbox"/></p> | <p>For IPv4 addresses</p> | <ol style="list-style-type: none"> 1. Navigate to the OA1 IPv4 and click OK. 2. On the OA1 Network Mode screen, select Static and click OK. 3. Select Accept and click OK. 4. On the Change:OA1 IP address screen, fill in data below, and click OK. <ul style="list-style-type: none"> • IP • MASK • gateway 5. Select Accept and click OK. 6. Navigate to OA2 IP menu setting on the Insight display and repeat the above steps to assign the IP parameters of OA2. |
| <p>4. <input type="checkbox"/></p> | <p>For IPv6 addresses</p> | <ol style="list-style-type: none"> 1. Navigate to the OA1 IPv6 and click OK. 2. On the Change: OA1 IPv6 Status menu, select the Enabled option and click OK. 3. Select Accept and click OK. 4. On the Change:OA1 IPv6 Settings screen, fill in appropriate data, and click OK. <ol style="list-style-type: none"> a. Set the Static IPv6 address to the globally scoped address and prefix and click OK. b. If not already disabled, set the DHCPv6 option to Disabled. c. If not already disabled, set the SLAAC option to Disabled. d. If a static Gateway address is to be configured, navigate to Static Gateway, and click OK. <ul style="list-style-type: none"> • Select the Static Gateway IPv6 Address and click OK. • Select Set and click OK. e. Navigate to OA2 IP menu setting on the Insight display and repeat the above steps to assign the IP parameters of OA2. f. Select Accept All and click OK. <p>The Main Menu displays.</p> |

7.2 Configure Initial OA Settings Using the Configuration Wizard

This procedure configures initial OA settings using a configuration wizard. This procedure should be used for initial configuration only and should be executed when the onboard administrator in OA Bay 1 (left as viewed from rear) is installed and active.

Prerequisites:

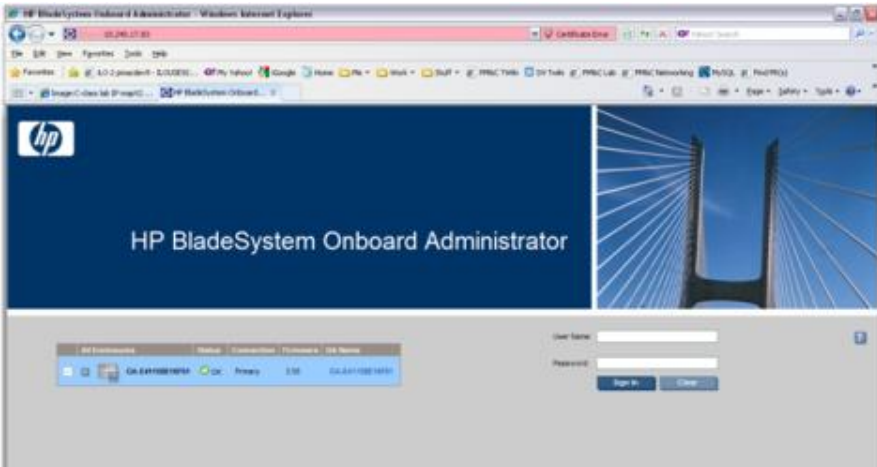
- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.
- 7.1 Configure Initial OA IP
- Both OAs are installed

Notes:

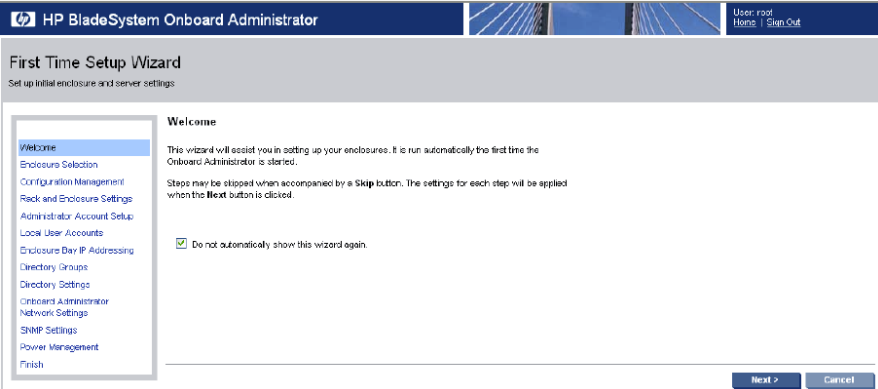

- The enclosure should be provisioned with two onboard administrators. The OA in Bay 2 automatically acquires its configuration from the OA in Bay 1 after the configuration is complete.
- Use this procedure for initial configuration only. Follow 7.7 Replace Onboard Administrator to learn how to replace one of the onboard administrators correctly.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

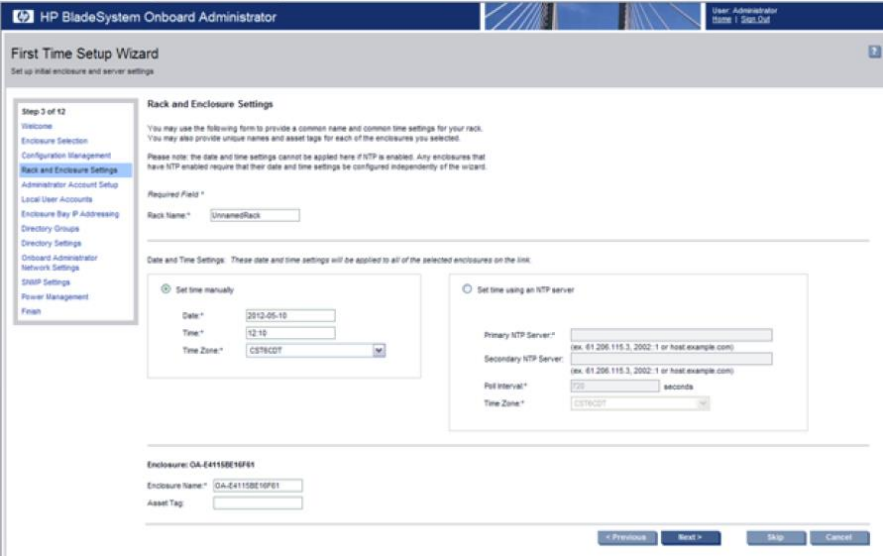
Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|------------------------------------|-----------------------------|--|
| <p>1. <input type="checkbox"/></p> | <p>OA GUI: Login</p> | <p>From a web browser, navigate to the OA Bay1 IP address assigned in 7.1 Configure Initial OA IP.</p> <p><code>http://<OA_IP></code></p> <p>Login as an administrative user. The original password is on a paper card attached to each OA.</p>  |

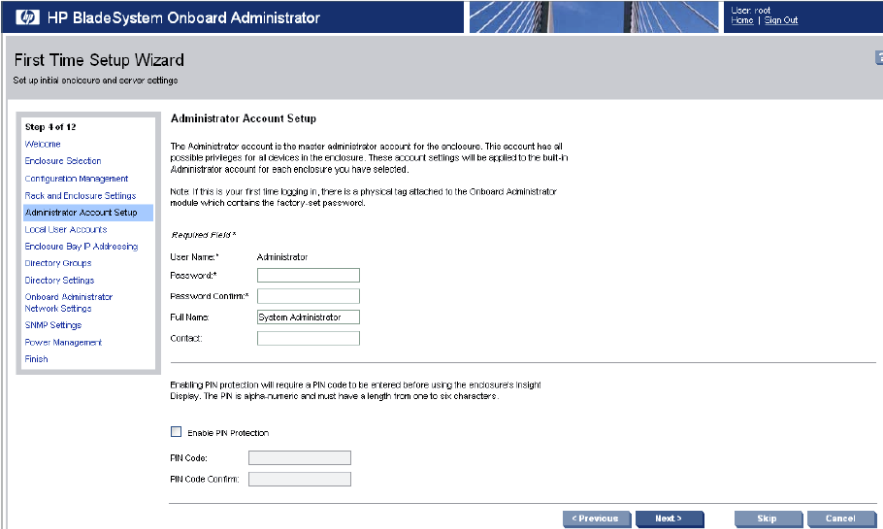
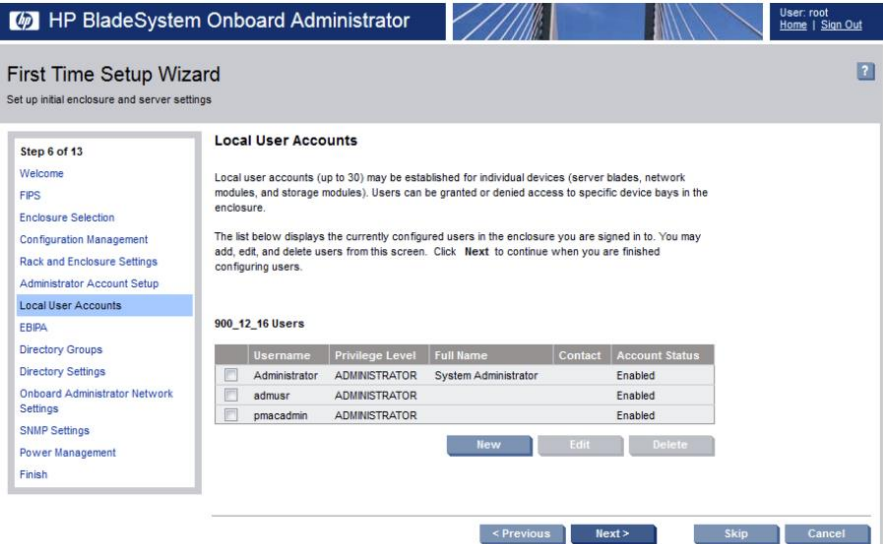
Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|------------------------------------|---|--|
| <p>2. <input type="checkbox"/></p> | <p>OA GUI: Run First Time Setup Wizard</p> | <p>Run the First Time Setup Wizard.</p>  <p>If needed, navigate to Wizards > First Time Setup.</p> |
| <p>3. <input type="checkbox"/></p> | <p>OA GUI: Select the enclosure</p> | <p>Click Next to select the enclosure to configure.</p>  |
| <p>4. <input type="checkbox"/></p> | <p>OA GUI: FIPS screen</p> | <p>Click Next. FIPS mode is not currently supported.</p> |
| <p>5. <input type="checkbox"/></p> | <p>OA GUI: Enclosure Selection screen</p> | <p>Click Next and select the enclosure.</p> |
| <p>6. <input type="checkbox"/></p> | <p>OA GUI: Configuration Management screen</p> | <p>Click Next. Skip Configuration management.</p> |

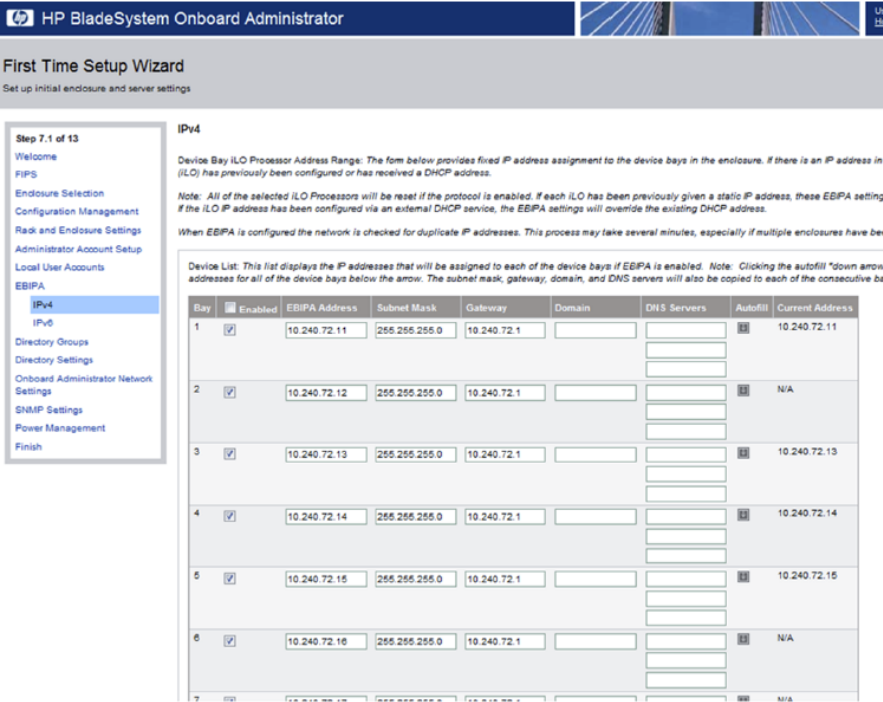
Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|---|--|--|
| <p>7.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Rack and Enclosure Settings screen</p> | <p>Click Next and type:</p> <ul style="list-style-type: none"> • The Rack Name in format xxx_xx. • The Enclosure Name in format <rack name>_<position> <p>Example:</p> <p>Rack Name: 500_03 Enclosure Name: 500_03_03</p> <p>Note: Enclosure positions are numbered from 1 at the bottom of the rack to 4 at the top.</p> <ul style="list-style-type: none"> • Mark the Set time using an NTP server option. • Type the Primary NTP Server, which is recommended to be set to the <customer_supplied_ntp_server_address>). • Set Poll Interval to 720. • Set Time Zone to UTC, if the customer does not have any specific requirements.  <p>The screenshot shows the 'First Time Setup Wizard' interface. On the left is a navigation pane with 'Rack and Enclosure Settings' selected. The main area is titled 'Rack and Enclosure Settings' and contains a 'Required Field' section with a 'Rack Name' input field. Below this is the 'Date and Time Settings' section, which has two radio buttons: 'Set time manually' and 'Set time using an NTP server'. The 'Set time manually' section has fields for Date (2012-05-10), Time (12:10), and Time Zone (CST/CDT). The 'Set time using an NTP server' section has fields for Primary NTP Server, Secondary NTP Server, Poll Interval (720 seconds), and Time Zone (CST/CDT). At the bottom, there are fields for Enclosure Name (OA-E4115BE10F01) and Asset Tag. Navigation buttons for Previous, Next, Skip, and Cancel are at the bottom right.</p> |

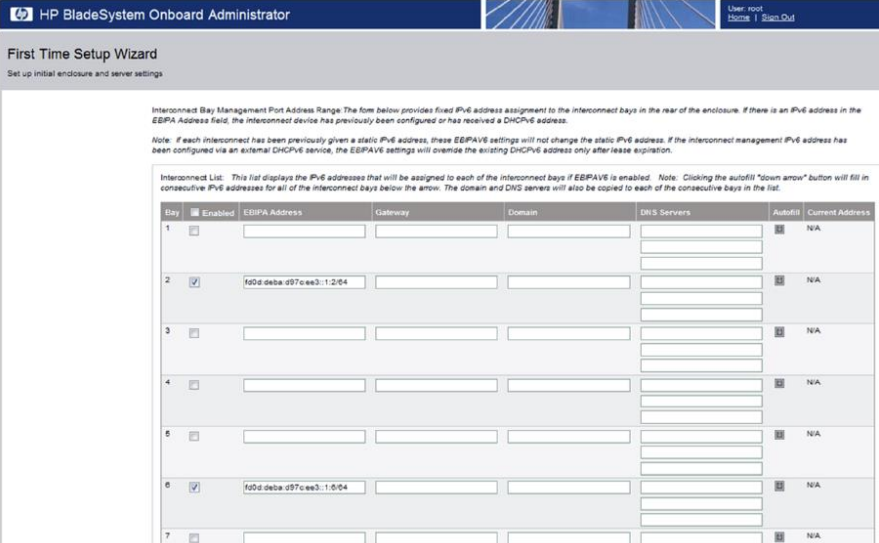
Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>8. <input type="checkbox"/></p> | <p>OA GUI: Administrator Account Setup screen</p> | <p>Click Next and change the administrator password.</p>  |
| <p>9. <input type="checkbox"/></p> | <p>OA GUI: Configure EBIPA settings</p> | <p>Click Next to create the pmacadmin and admusr user.</p> <ul style="list-style-type: none"> On the Local User Accounts screen, click New to add pmacadmin user. Type the User Name and Password. Set the Privilege Level to Administrator. Refer to the application documentation for the password. Verify all of the blades have been checked before marking the Onboard Administrator Bays checkbox under the User Permissions section. Click Add User. Repeat to create the admusr user.  |

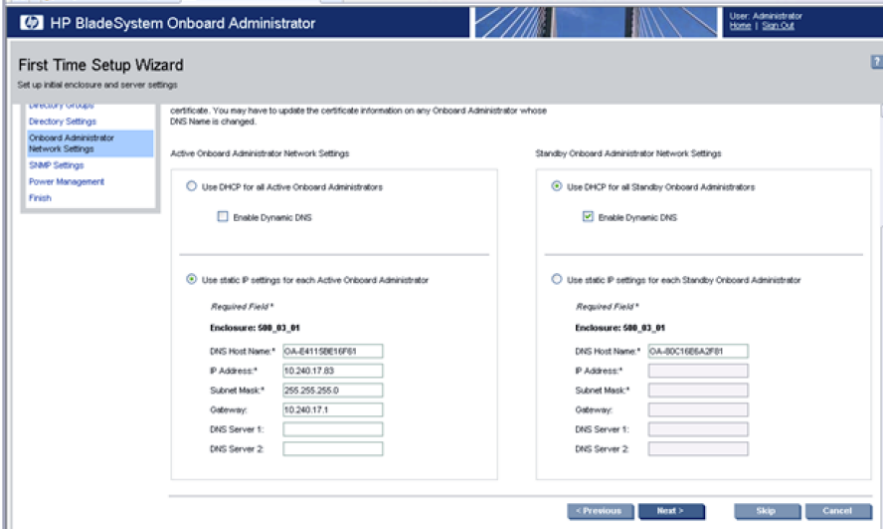
Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|--|---|---|
| <p>10.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Enclosure Bay IP Addressing</p> | <p>Click Next to configure the EBIPA settings. Click Next to continue or Skip if the EBIPA has been configured. Note: The EBIPA address setup is required.</p> <p>1. For IPv4, click First Time Setup Wizard EBIPA: IPv4.</p> <p>a. From the Device List pane, type the iLO IP Address, Subnet Mask, and Gateway fields for device bays 1-16.</p> <p>Do not fill in the iLO IP Address, Subnet Mask, and Gateway fields for device bays 1A-16A or 1B-16B.</p> <p>Note: Bays 1A-16A and 1B-16B are used for double-density blades, for example, BL2x220c, which are not supported in this release.</p> <p>b. Click Enabled for each device bay 1 through 16 in use.</p> <p>Notes:</p> <ul style="list-style-type: none"> Any unused slots should have an IP address assigned, but should not be disabled. Do not use autofill as this will fill the entries for the Device Bays 1A through 16B.  <p>c. Scroll to the Interconnect List (below Device Bay 16B).</p> <p>d. Type the EBIPA Address, Subnet Mask, and Gateway fields for each Interconnect Bay in use.</p> <p>e. Click Enable for each Interconnect Bay in use.</p> |

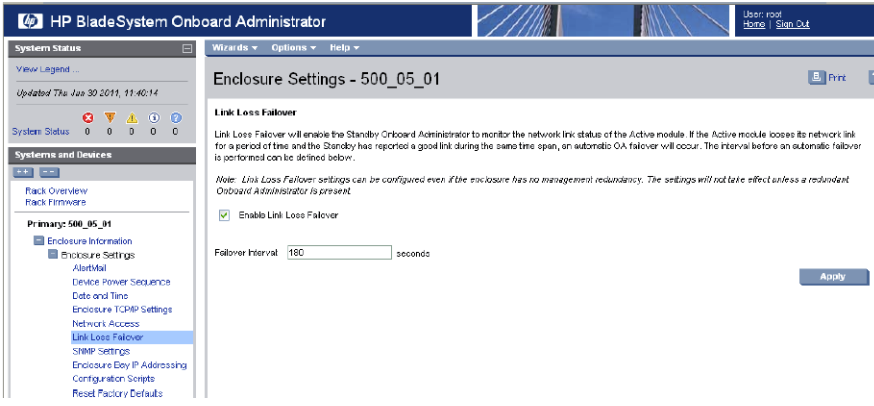
Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|------|-----------|--|
| | | <p>f. Click Next to apply settings.</p> <p>The system may restart devices such as interconnect devices or iLOs to apply new addresses.</p> <p>g. Check the IP address to ensure the settings are correct.</p> <p>2. For IPv6, click First Time Setup Wizard EBIPA: IPv6.</p> <p>a. From the Device List pane, type the iLO IP Address/Prefix or Gateway fields for device bays 1-16.</p> <p>Do not fill in the iLO IP Address/Prefix and Gateway fields for device bays 1A-16A or 1B-16B.</p> <p>Note: Bays 1A-16A and 1B-16B are used for double-density blades, for example, BL2x220c, which are not supported in this release.</p> <p>b. Click Enabled for each device bay 1 through 16 in use.</p> <p>Notes:</p> <ul style="list-style-type: none"> Any unused slots should have an IP address assigned, but should not be disabled. Do not use autofill as this will fill the entries for the Device Bays 1A through 16B.  <p>c. Scroll to the Interconnect List (below Device Bay 16B).</p> <p>d. Type the EBIPA Address/Prefix and Gateway fields for each Interconnect Bay in use.</p> <p>e. Click Enable for each Interconnect Bay in use.</p> <p>f. Click Next to apply settings.</p> <p>The system may restart devices such as interconnect devices or iLOs to apply new addresses.</p> <p>g. Check the IP address to ensure the settings are correct.</p> |

Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|---------------------------------|---|---|
| 11. <input type="checkbox"/> | OA GUI: Directory Groups screen | Skip Directory Group setup. |
| 12. <input type="checkbox"/> | OA GUI: Directory Settings screen | Click Next . Skip Directory Settings setup. |
| 13. <input type="checkbox"/> | OA GUI: Onboard Administrator Network Settings screen | <p>Click Next.</p> <p>On the Onboard Administrator Network Settings screen, you can assign or modify the IP address and the other network settings for the Onboard Administrator(s).</p> <p>The Active Administrator Network Settings pertain to the active OA (OA Bay 1 location during initial configuration). If the second Onboard Administrator is present, the Standby Onboard Administrator Network Settings also display.</p> <ol style="list-style-type: none"> 1. Click Use static IP settings for each Standby Onboard Administrator. 2. Type the IP Address, Subnet Mask, and Gateway for the standard OA.  <ol style="list-style-type: none"> 3. Click Next. <p>If you changed the IP address of the active OA, you are disconnected. Close your browser and login again using the new IP address.</p> |
| 14. <input type="checkbox"/> | OA GUI: SNMP Settings screen | <p>By default, the Enable SNMP checkbox is marked. If you do not want to have SNMP enabled, see Appendix I Disable SNMP on the OA.</p> <p>Note: This step does not set an SNMP Trap Destination. To do this, see 7.10 Add SNMP Trap Destination on OA.</p> |

Procedure 44. Configure Initial OA Settings Using the Configuration Wizard

| Step | Procedure | Results |
|---------------------------------|---|--|
| 15. <input type="checkbox"/> | OA GUI: Power Management screen | Click Next . The Power Mode setting on the Power Management screen must be configured for power supply redundancy. The first available setting on the Power Management screen is either AC Redundant or Redundant , depending on whether the Enclosure is powered by AC or DC. In either case, click Power Supply Redundant option. For all other settings on the Power Management screen, leave the default settings unchanged. |
| 16. <input type="checkbox"/> | OA GUI: Finish screen | Click Next . Click Finish . |
| 17. <input type="checkbox"/> | OA GUI: Set link loss failover | Navigate to Enclosure Information > Enclosure Settings > Link Loss Failover . Mark the Enable Link Loss Failover checkbox and specify the Failover Interval to be 180 seconds. Click Apply .  |

7.3 Configure OA Security

This procedure disables telnet access to OA.

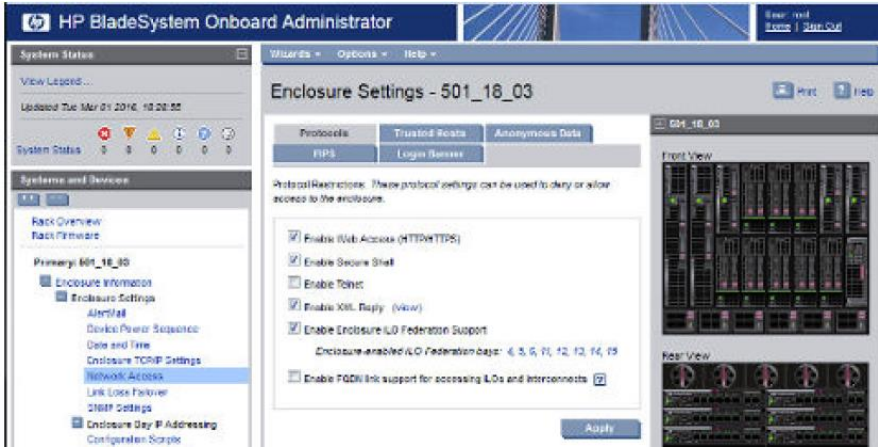
Prerequisite: 7.2 Configure Initial OA Settings Using the Configuration Wizard

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 45. Configure OA Security

| Step | Procedure | Results |
|--------------------------------|----------------------|---|
| 1. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |

Procedure 45. Configure OA Security

| Step | Procedure | Results |
|--------------------------------|----------------------------------|---|
| 2. <input type="checkbox"/> | OA GUI: Disable telnet | <ol style="list-style-type: none"> Navigate to Enclosure Information > Enclosure Settings > Network Access. Unmark the Enable Telnet checkbox.  |
| 3. <input type="checkbox"/> | OA GUI: Apply changes | Click Apply . |

7.4 Upgrade or Downgrade OA Firmware

If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP.

This procedure upgrades or downgrades the firmware on the OAs. The procedure also ensures both OAs have the same firmware version. When the firmware update begins, the standby OA automatically updates first.

Prerequisite: Obtain customer approval needed for OA firmware updates. This procedure can change the version of firmware installed in one or both OAs.

Needed Material

- HP MISC firmware ISO image
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

Note: The enclosure should be provisioned with two onboard administrators. This procedure installs the same firmware version on both onboard administrators.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6.x is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

7.5 Store OA Configuration on Management Server

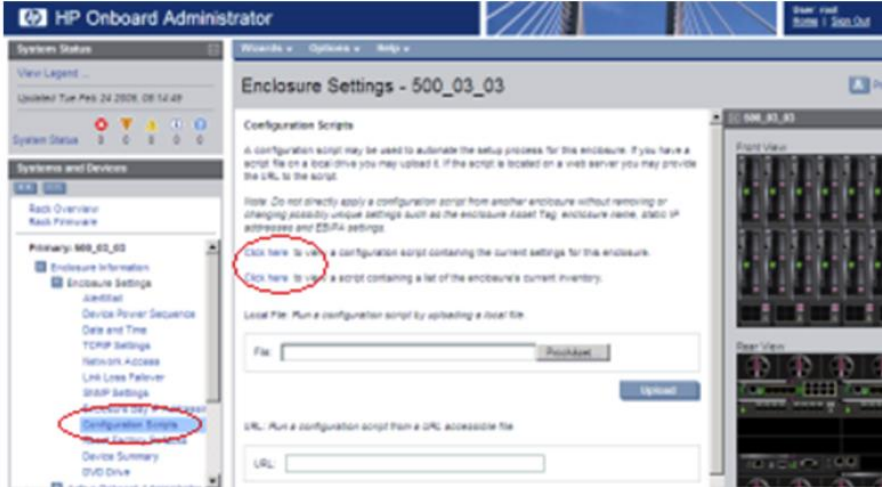
This procedure backs up OA settings on the management server.

Prerequisites:

- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 46. Store OA Configuration on Management Server

| Step | Procedure | Results |
|---------|---|--|
| 1. □ | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |
| 2. □ | OA GUI: Store configuration file | <ol style="list-style-type: none"> 1. Navigate to Enclosure Information > Enclosure Settings > Configuration Scripts. 2. Open the first configuration file (current settings for enclosure).  <ol style="list-style-type: none"> 3. Store file on the local disk. 4. Click Show Config. <p>Copy all text on the screen and save it in a text file or navigate to File > Save As and select a filename and path. Select Text file as the type.</p> <p>For example, you may select the following syntax for the configuration file name:</p> <pre><enclosure ID>_<timetag>.conf</pre> |

Procedure 46. Store OA Configuration on Management Server

| Step | Procedure | Results |
|-----------------|--|---|
| <p>3. □</p> | <p>PMAC: Back up configuration file</p> | <ol style="list-style-type: none"> 1. Under <code>/usr/TKLC/smac/etc</code> directory, you can create your own subdirectory structure. Log into the management server using ssh as admusr and create the target directory: <pre>\$ sudo /bin/mkdir -p /usr/TKLC/smac/etc/OA_backups/OABackup</pre> 2. Change the directory permissions: <pre>\$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/OA_backups \$ sudo /bin/chmod go+x /usr/TKLC/smac/etc/OA_backups/OABackup \$ sudo /bin/chown pmacd:pmacbackup /usr/TKLC/smac/etc/OA_backups \$ sudo /bin/chown pmacd:pmacbackup /usr/TKLC/smac/etc/OA_backups/OABackup</pre> 3. Copy the configuration file to the created directory. <p>For UNIX users:</p> <pre># scp ./<cabinet_enclosure_backup file>.conf \ admusr@<pmac_management_network_ip>:/home/admsr</pre> <p>Windows users:</p> <p>Refer to Appendix A Using WinSCP to copy the file to the management server.</p> 4. On the PMAC, move the configuration file to the OA Backup folder you created under <code>/usr/TKLC/smac/etc</code>: <pre>\$ sudo /bin/mv /home/admsr/<cabinet_enclosure_backup file>.conf /usr/TKLC/smac/etc/OA_backups/OABackup</pre> |
| <p>4. □</p> | <p>PMAC: Use PMAC application backup to capture the OA backup</p> | <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm backup PMAC backup been successfully initiated as task ID 7</pre> <p>Notes:</p> <ul style="list-style-type: none"> • The backup runs as a background task. To check the status of the background task, use the PMAC GUI Task Monitor screen, or the command <code>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</code>. The result should eventually be PMAC Backup successful and the background task should indicate COMPLETE. • The <code>pmacadm backup</code> command uses a naming convention that includes a date/time stamp in the file name (for example: <code>backupPmac_20111025_100251.pef</code>). In the example, the backup file name indicates it was created on 10/25/2011 at 10:02:51 am server time. |

Procedure 46. Store OA Configuration on Management Server

| Step | Procedure | Results |
|--|--|---|
| <p>5. <input type="checkbox"/></p> | <p>PMAC: Verify backup was successful</p> | <p>If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact Error! Bookmark not defined..</p> <p>The output of <code>pmaccli getBgTasks</code> should look similar to this:</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks 2: Backup PMAC COMPLETE - PMAC Backup successful Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum: 2 Server Identity: Physical Blade Location: Blade Enclosure: Blade Enclosure Bay: Guest VM Location: Host IP: Guest Name: TPD IP: Rack Mount Server: IP: Name: ::</pre> |
| <p>6. <input type="checkbox"/></p> | <p>PMAC: Save the backup</p> | <p>If the NetBackup feature has not been configured for this PMAC or the Redundant PMAC is not configured in this system, the PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility) the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the <code>/var/TKLC/smac/backup</code> directory.</p> |
| <p>7. <input type="checkbox"/></p> | <p>OA GUI: Log out</p> | <p>Log out from the OA by clicking Sign Out at the top right corner.</p> |

7.6 Restore OA Configuration from Management Server

This procedure restores configuration backup from the management server and applies it on the OAs.

Prerequisites:

- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.
- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- 9.3 Deploy PMAC Guest

It is assumed that:

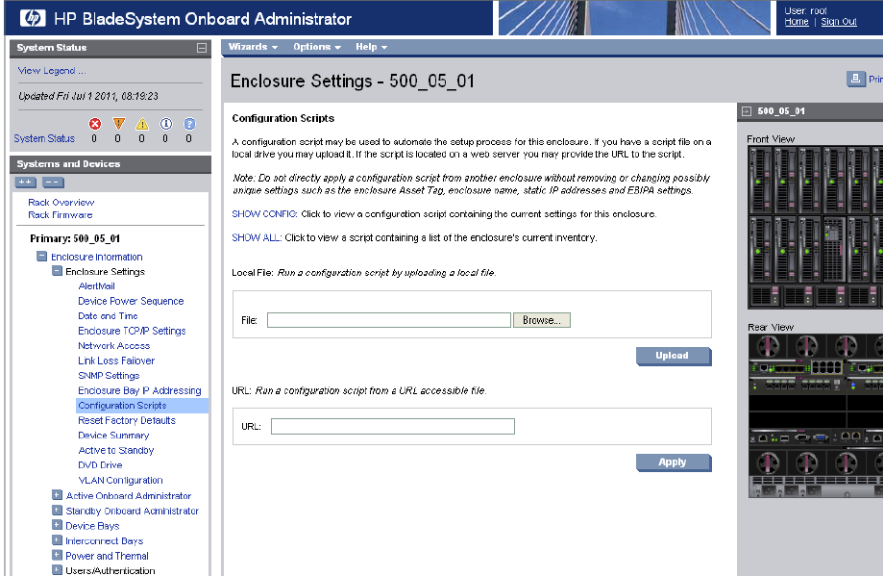
- 7.5 Store OA Configuration on Management Server has already been performed.
- 7.1 Configure Initial OA IP has been completed before this procedure.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 47. Restore OA Configuration from Management Server

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Obtain configuration files from the management server | <ol style="list-style-type: none"> 1. Log into the PMAC server as the admusr user. 2. Copy the OA backup file to the home directory of admusr: <pre>\$ sudo cp /usr/TKLC/smac/etc/OA_backups/OABackup/<backup_config_filename> /home/admusr</pre> 3. Make the file readable by admusr: <pre>\$ sudo chown admusr /home/admusr/<backup_config_filename> \$ sudo chmod 400 /home/admusr/<backup_config_filename></pre> 4. From the PC, use scp or WinSCP to copy the file from admusr@<PMAC IP>:/home/admusr/<backup_config_filename> <p>Unix Users:</p> <pre>\$ scp admusr@<pmac_management_network_ip>:/usr/TKLC/smac/etc/OA_backups/OABackup/<backup_config_filename> .</pre> <p>Windows Users:</p> <p>Refer to Using WinSCP to copy the file to your PC.</p> 5. On the PMAC, remove the file copied above: <pre>\$ sudo rm /home/admusr/<backup_config_filename></pre> 6. Log out of the PMAC server. |
| 2. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |

Procedure 47. Restore OA Configuration from Management Server

| Step | Procedure | Results |
|---|---|---|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Restore configuration</p> | <ol style="list-style-type: none"> Navigate to Enclosure Information > Enclosure Settings > Configuration Scripts. Use Local file to upload and run the configuration script.  <p>The restore can take 5-10 minutes.</p> <p>A screen displays when the restore is complete that contains logs from the restoration process. Make sure there are no errors.</p> <p>Note If both OAs were reset to factory defaults and have to be restored from the configuration file, the configured user's passwords must be manually reset to their original values. Specifically, the pmacadmin user password so the PMAC and the OAs can communicate.</p> |
| <p>4.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Log out</p> | <p>Log out from the OA by clicking Sign Out at the top right corner.</p> |

7.7 Replace Onboard Administrator

This procedure replaces OA in an enclosure with redundant OA.

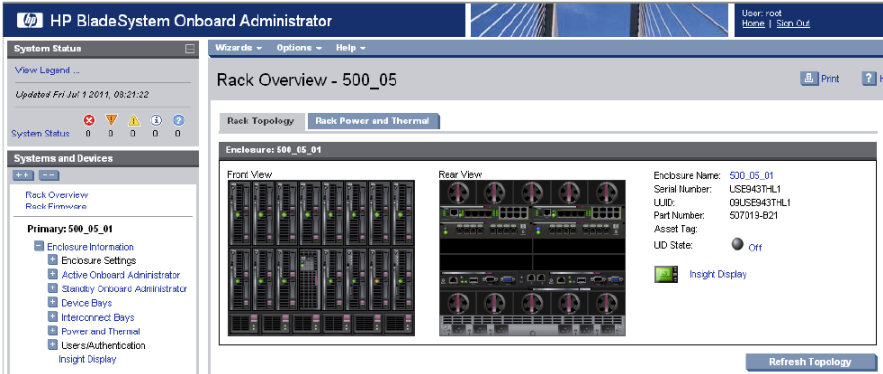
Prerequisites:

- Obtain customer approval needed for OA firmware updates. This procedure can change the version of firmware installed in one or both OAs.
- If the aggregation switches are supported by Oracle, then the Cisco 4948/4948E/4948E-F switches must be configured using 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig). If the aggregation switches are provided by the customer, ensure the switches are configured as per requirements provided in the NAPD. If there is any doubt as to whether the aggregation switches are provided by Oracle or the customer, contact **Error! Bookmark not defined.** for assistance.
- 7.3 Configure OA Security

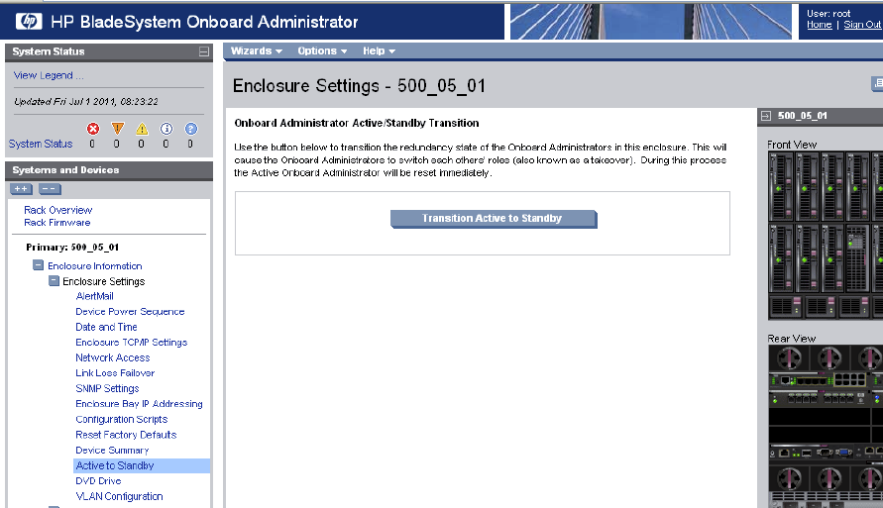
Note: The transfer of configuration occurs only from OA in Bay 1 to OA in Bay 2. Therefore, to keep the current configuration of the system, the insertion of new OA into the OA Bay 1 location should be avoided.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 48. Replace Onboard Administrator

| Step | Procedure | Results | | | | | | | | | | | | |
|--|---|---|--|--------|---------|---------------|--|--|----------------|--|--|------------|--|--|
| <p>1. <input type="checkbox"/></p> | <p>OA GUI: Login</p> | <p>Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as root.</p>  | | | | | | | | | | | | |
| <p>2. <input type="checkbox"/></p> | <p>OA GUI: Record the IP configuration of the active and standby OAs</p> | <ol style="list-style-type: none"> 1. Navigate to Enclosure Information > Active Onboard Administrator > TCP/IP Settings. 2. Record the Active OA's IP Address, Subnet Mask, and Gateway. 3. Navigate to Enclosure Information > Standby Onboard Administrator > TCP/IP Settings. 4. Record the Standby OA's IP Address, Subnet Mask, and Gateway. <table border="1" data-bbox="505 1167 1425 1360"> <thead> <tr> <th></th> <th>Active</th> <th>Standby</th> </tr> </thead> <tbody> <tr> <td>OA IP Address</td> <td></td> <td></td> </tr> <tr> <td>OA Subnet Mask</td> <td></td> <td></td> </tr> <tr> <td>OA Gateway</td> <td></td> <td></td> </tr> </tbody> </table> | | Active | Standby | OA IP Address | | | OA Subnet Mask | | | OA Gateway | | |
| | Active | Standby | | | | | | | | | | | | |
| OA IP Address | | | | | | | | | | | | | | |
| OA Subnet Mask | | | | | | | | | | | | | | |
| OA Gateway | | | | | | | | | | | | | | |
| <p>3. <input type="checkbox"/></p> | <p>OA GUI: Note the location of the active OA</p> | <p>Note the location of the active onboard administrator within the enclosure. The active OA has the active LED on. You may also hover over the OA to see its role.</p> <p>If the OA to be replaced is not the active OA for the enclosure, skip to step 5. ; otherwise, continue with the next step.</p> | | | | | | | | | | | | |

Procedure 48. Replace Onboard Administrator

| Step | Procedure | Results |
|--|--|--|
| <p>4.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Force active OA into standby mode</p> | <p>1. Navigate to Enclosure Information > Enclosure Settings > Active to Standby and click Transition Active to Standby.</p>  <p>2. Click OK when it asks if you are sure.</p> <p>3. Wait about five minutes until the application reloads and login screen displays.</p> |
| <p>5.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Remove the OA to be replaced</p> | <p>If you need to replace the Onboard Administrator from the OA Bay 2 location (right as viewed from rear) , remove it and skip to step 7.</p> <p>If you need to replace the Onboard Administrator from the OA Bay 1 location (left as viewed from rear), remove it, and proceed with the next step.</p> |
| <p>6.</p> <p><input type="checkbox"/></p> | <p>OA GUI</p> | <p>Move the OA from OA Bay 2 location into the OA Bay 1 location.</p> <p>Wait five minutes so the Onboard Administrator can initialize.</p> |
| <p>7.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Install the new OA</p> | <p>Insert the new Onboard Administrator into OA Bay 2 of the enclosure and wait five minutes so it can get its configuration from the other OA and initialize.</p> |
| <p>8.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Login</p> | <p>Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator.</p> |
| <p>9.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Re-establish the OA's IP configuration</p> | <p>Refer to the OA IP configuration settings recorded in step 2. of this procedure. The current settings of each OA should be unique and should match the recorded settings for either the active or standby OA. The active OA may now have the standby OA's recorded settings and vice versa. If changes are needed, perform 7.1 Configure Initial OA IP.</p> |
| <p>10.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Verify the status of the OA</p> | <p>On the Rear View, hover over each OA and verify the Status is OK. If the status of one OA or the other is shown as Degraded because of a firmware version mismatch, perform 7.4 Upgrade or Downgrade OA Firmware.</p> |

Procedure 48. Replace Onboard Administrator

| Step | Procedure | Results |
|---------------------------------|--|--|
| 11. <input type="checkbox"/> | PMAC CLI: Delete OA SSH keys | Log into the PMAC CLI as admusr. Execute these three commands: <pre>\$ sudo /usr/bin/ssh-keygen -R <Active-OA-IP> -f ~pmacd/.ssh/known_hosts</pre> <pre>\$ sudo /usr/bin/ssh-keygen -R <Standby-OA-IP> -f ~pmacd/.ssh/known_hosts</pre> <pre>\$ sudo /bin/chown pmacd:pmacd ~pmacd/.ssh/known_hosts</pre> PMAC established new SSH keys the next time it logs into each OA. |

7.8 Update IPv4 Address

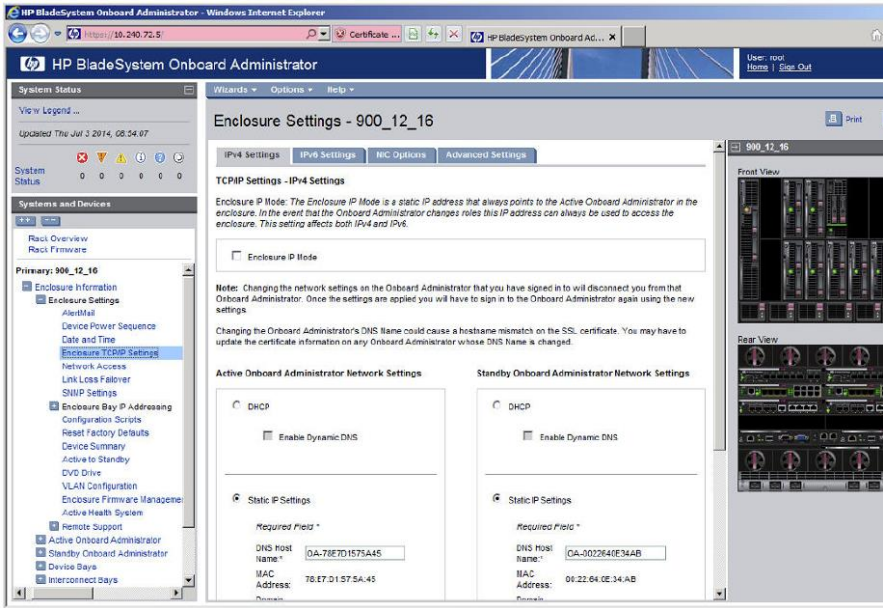
This procedure updates the IP address for a C7000 enclosure.

Prerequisites:

- Obtain address information from the customer.
- The enclosure has been previously configured and the PMAC GUI is reachable over the network.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.


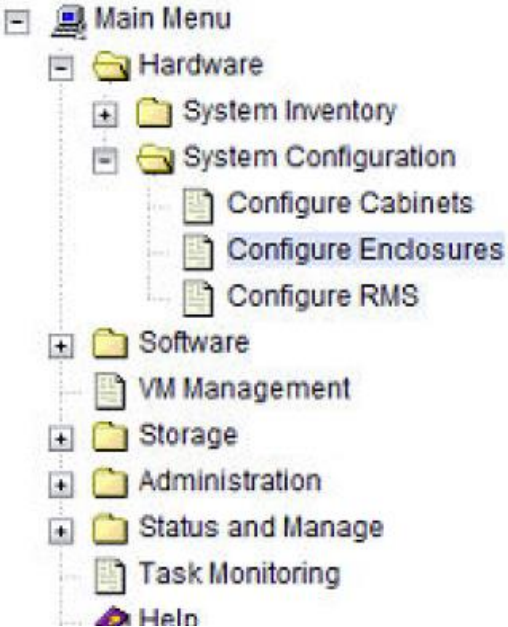
Procedure 49. Update IPv4 Address

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |
| 2. <input type="checkbox"/> | OA GUI: Update the IPv4 OA settings | Navigate to Enclosure Information > Enclosure Settings > Enclosure TCP/IP Settings.  |

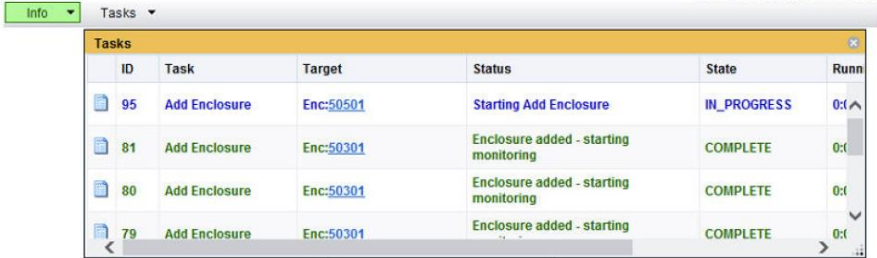
Procedure 49. Update IPv4 Address

| Step | Procedure | Results |
|--|--|--|
| <p>3. <input type="checkbox"/></p> | <p>OA GUI: Update the static IP settings for both active and standby OA</p> | <p>Change the:</p> <ul style="list-style-type: none"> • IP Address • Subnet Mask • Gateway <p>Click Apply.</p> |
| <p>4. <input type="checkbox"/></p> | <p>OA GUI: Update the EBIPA settings</p> | <p>4. Navigate to Enclosure Information > Enclosure Settings > Enclosure Bay IP Addressing > IPv4 > Device Bays tab.</p> <p>5. Update the IP settings for the device bays by changing:</p> <ol style="list-style-type: none"> a. EBIPA Address b. Subnet Mask c. Gateway <p>6. Click Apply.</p> <p>7. Select the Interconnect Bays tab and update the IP settings for the interconnect device bays by changing:</p> <ol style="list-style-type: none"> a. EBIPA Address b. Subnet Mask c. Gateway <p>8. Click Apply.</p> |
| <p>5. <input type="checkbox"/></p> | <p>OA GUI: Log out</p> | <p>Log out from the OA by clicking Sign Out at the top right corner.</p> |

Procedure 49. Update IPv4 Address

| Step | Procedure | Results |
|-----------------|--|---|
| <p>6. □</p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guidadmin user.</p>  <p>Navigate to Main Menu > Hardware > System Configuration > Configure Enclosures.</p>  |
| <p>7. □</p> | <p>PMAC GUI: Select the enclosure to edit</p> | <p>On the Configure Enclosures panel, select the enclosure you are modifying and click Edit Enclosure.</p> |

Procedure 49. Update IPv4 Address

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|--|---|---------------------------------------|-------------|--------|--------|-------|------|----|---------------|-----------|------------------------|-------------|-----|----|---------------|-----------|---------------------------------------|----------|-----|----|---------------|-----------|---------------------------------------|----------|-----|----|---------------|-----------|----------------------------|----------|-----|
| 8. <input type="checkbox"/> | PMAC GUI: Edit the enclosure address | <p>On the Edit Enclosure panel, update the IP addresses, and click Edit Enclosure.</p> <p>The screen refreshes with a new background task entry. Click Tasks located on the toolbar under the Configure Enclosures heading.</p> <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures [Edit Enclosure 50501] Tue Sep 01 20:18:46 2015 UTC</p>  <p>The screenshot shows a 'Tasks' window with the following data:</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Runn</th> </tr> </thead> <tbody> <tr> <td>95</td> <td>Add Enclosure</td> <td>Enc:50501</td> <td>Starting Add Enclosure</td> <td>IN_PROGRESS</td> <td>0:t</td> </tr> <tr> <td>81</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> <td>0:t</td> </tr> <tr> <td>80</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> <td>0:t</td> </tr> <tr> <td>79</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Enclosure added - starting</td> <td>COMPLETE</td> <td>0:t</td> </tr> </tbody> </table> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> | ID | Task | Target | Status | State | Runn | 95 | Add Enclosure | Enc:50501 | Starting Add Enclosure | IN_PROGRESS | 0:t | 81 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 0:t | 80 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 0:t | 79 | Add Enclosure | Enc:50301 | Enclosure added - starting | COMPLETE | 0:t |
| ID | Task | Target | Status | State | Runn | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 95 | Add Enclosure | Enc:50501 | Starting Add Enclosure | IN_PROGRESS | 0:t | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 81 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 0:t | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 0:t | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | Add Enclosure | Enc:50301 | Enclosure added - starting | COMPLETE | 0:t | | | | | | | | | | | | | | | | | | | | | | | | | | | |

7.9 Update IPv6 Address

This procedure updates the IP address for a C7000 enclosure. It can be used to add IPv6 addresses or edit existing IPv6 addresses.

Prerequisites:

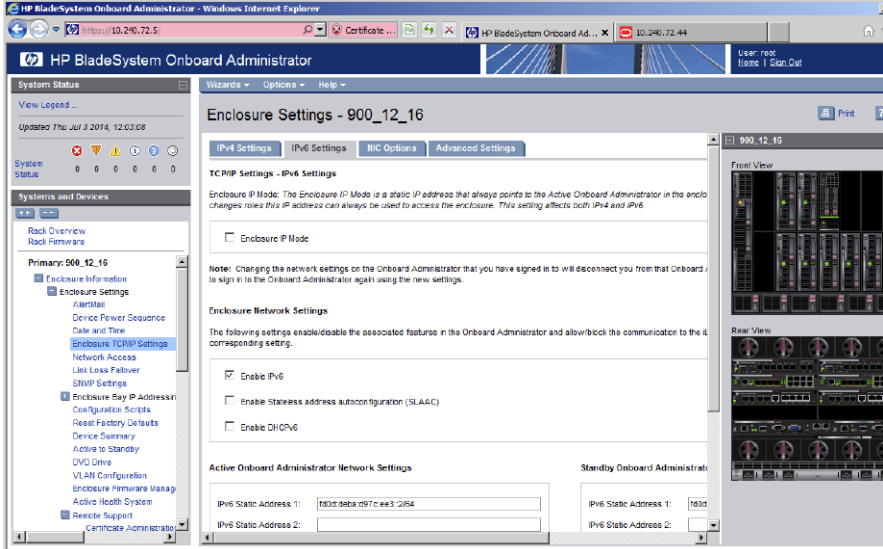
- Obtain address information from the customer.
- The enclosure has been previously configured and the PMAC GUI is reachable over the network.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.


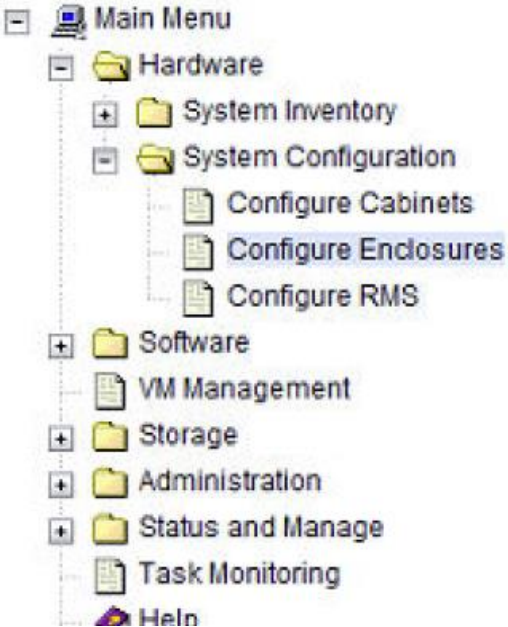
Procedure 50. Update IPv6 Address

| Step | Procedure | Results |
|--------------------------------|----------------------|---|
| 1. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |

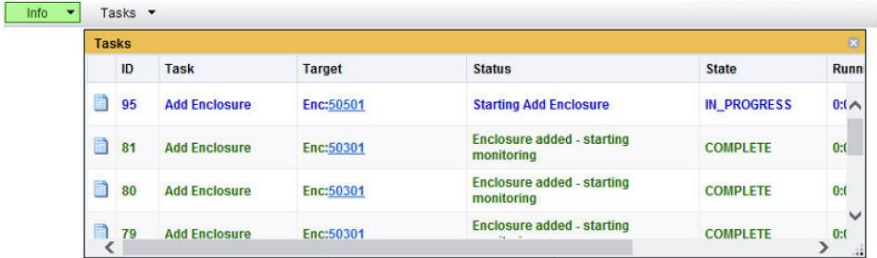
Procedure 50. Update IPv6 Address

| Step | Procedure | Results |
|------------------------------------|--|--|
| <p>2. <input type="checkbox"/></p> | <p>OA GUI: Update the IPv6 OA settings</p> | <p>Navigate to Enclosure Information > Enclosure Settings > Enclosure TCP/IP Settings IPv6 Settings tab.</p>  |
| <p>3. <input type="checkbox"/></p> | <p>OA GUI: Verify</p> | <p>Under Enclosure Network Settings, verify the Enable IPv6 checkbox is marked.</p> |
| <p>4. <input type="checkbox"/></p> | <p>OA GUI: Update the static IP settings for both active and standby OA</p> | <p>Change the:</p> <ul style="list-style-type: none"> • IPv6 Static Address a • Static Default Gateway <p>Click Apply.</p> |
| <p>5. <input type="checkbox"/></p> | <p>OA GUI: Update the EBIPA settings</p> | <ol style="list-style-type: none"> 1. Navigate to Enclosure Information > Enclosure Settings > Enclosure Bay IP Addressing > IPv6 > Device Bays tab. 2. Update the IP settings for the device bays by making sure Enabled is checked and changing: <ul style="list-style-type: none"> • EBIPA Address • Gateway 3. Click Apply. 4. Select the Interconnect Bays tab and update the IP settings for the interconnect device bays by making sure Enabled is checked and changing: <ul style="list-style-type: none"> • EBIPA Address • Gateway 5. Click Apply. |
| <p>6. <input type="checkbox"/></p> | <p>OA GUI: Log out</p> | <p>Log out from the OA by clicking Sign Out at the top right corner.</p> |

Procedure 50. Update IPv6 Address

| Step | Procedure | Results |
|-----------------|--|---|
| <p>7. □</p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guidadmin user.</p>  <p>Navigate to Main Menu > Hardware > System Configuration > Configure Enclosures.</p>  |
| <p>8. □</p> | <p>PMAC GUI: Select the enclosure to edit</p> | <p>On the Configure Enclosures panel, select the enclosure you are modifying and click Edit Enclosure.</p> |

Procedure 50. Update IPv6 Address

| Step | Procedure | Results |
|--------------------------------|--|--|
| 9. <input type="checkbox"/> | PMAC GUI: Edit the enclosure address | <p>On the Edit Enclosure panel, update the IP addresses, and click Edit Enclosure.</p> <p>The screen refreshes with a new background task entry. Click Tasks located on the toolbar under the Configure Enclosures heading.</p> <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures [Edit Enclosure 50501] Tue Sep 01 20:18:46 2015 UTC</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |

7.10 Add SNMP Trap Destination on OA

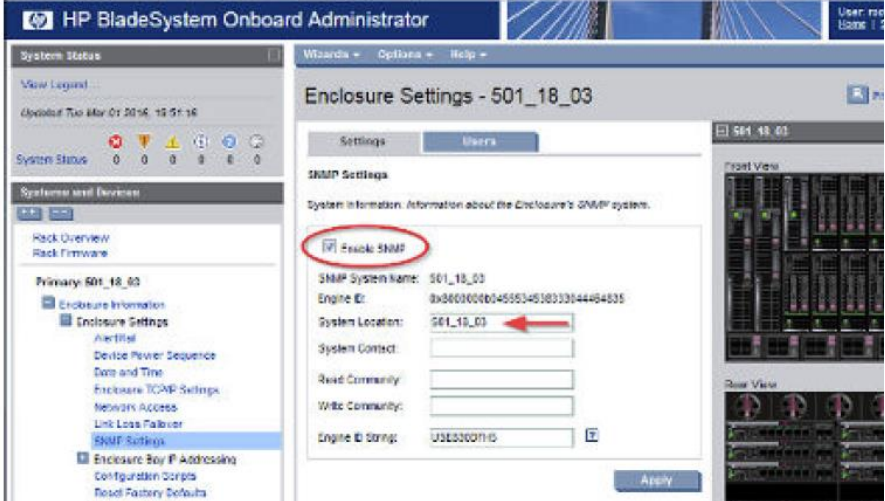
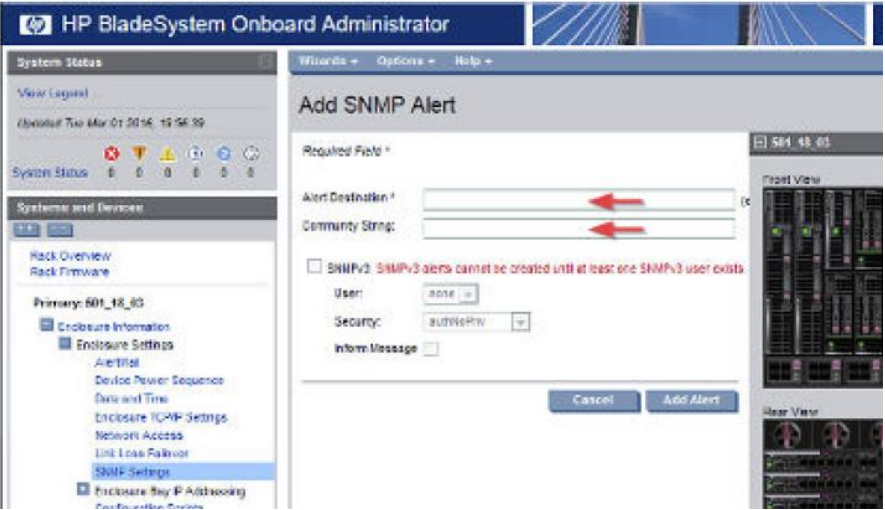
This procedure adds an SNMP trap destination and configures it using the OA.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 51. Add SNMP Trap Destination on OA

| Step | Procedure | Results |
|--------------------------------|----------------------|---|
| 1. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |

Procedure 51. Add SNMP Trap Destination on OA

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>2. <input type="checkbox"/></p> | <p>OA GUI: SNMP Setting screen</p> | <ol style="list-style-type: none"> Navigate to Enclosure Information > Enclosure Settings > SNMP Settings. If SNMP is not already enabled, mark the Enable SNMP checkbox. Type the enclosure name (shown in the title bar) or your preferred name as the System Location.  <p>Do not set Read Community and Write Community.</p> <ol style="list-style-type: none"> Click Apply. |
| <p>3. <input type="checkbox"/></p> | <p>OA GUI: Add SNMP alert destination</p> | <ol style="list-style-type: none"> Click New. Type the destination information into the Alert Destination box (for example, 61.206.115.3, 2002::1 or host.example.com). Type the Community String.  <ol style="list-style-type: none"> Click Add Alert. Repeat for each required destination. |

7.11 Disable SNMP Trap Destination on OA

This procedure disables an SNMP trap destination using the OA.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 52. Disable SNMP Trap Destination on OA

| Step | Procedure | Results |
|--------------------------------|------------------------------------|---|
| 1. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |
| 2. <input type="checkbox"/> | OA GUI: SNMP Setting screen | <ol style="list-style-type: none"> 1. Navigate to Enclosure Information > Enclosure Settings > SNMP Settings. 2. Unmark the Enable SNMP checkbox. 3. Click Apply. |

7.12 Delete SNMP Trap Destination on OA

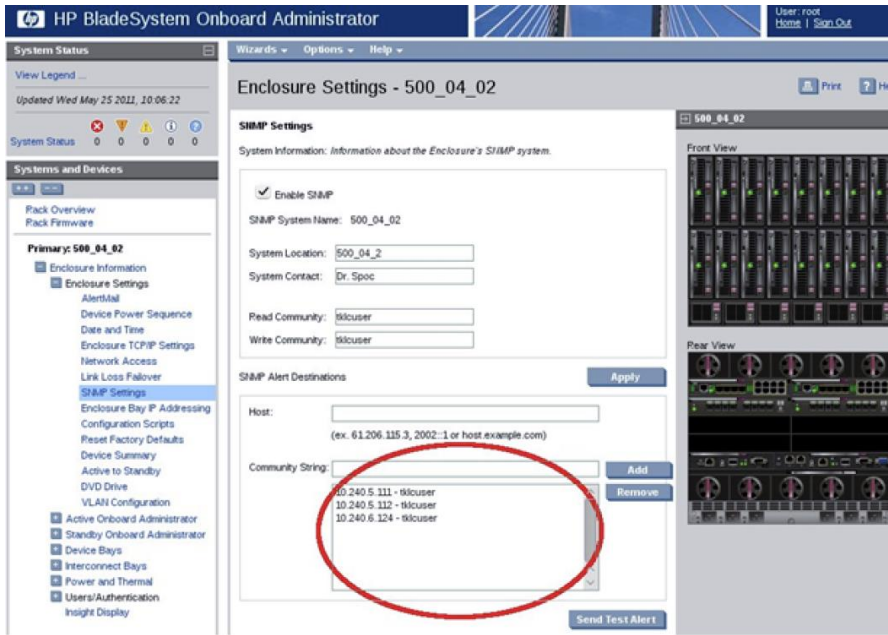
This procedure removes an SNMP trap destination from the OA.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 53. Delete SNMP Trap Destination on OA

| Step | Procedure | Results |
|--------------------------------|----------------------|---|
| 1. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |

Procedure 53. Delete SNMP Trap Destination on OA

| Step | Procedure | Results |
|------------------------------------|---|---|
| <p>2. <input type="checkbox"/></p> | <p>OA GUI: SNMP Setting screen</p> | <p>1. Navigate to Enclosure Information > Enclosure Settings > SNMP Settings.</p> <p>All configured SNMP trap destination display.</p> <p>2. Select the trap destination and click Remove.</p>  <p>If no SNMP trap destinations display, then you may want to disable SNMP by unmarking the Enable SNMP checkbox.</p> <p>3. Click Apply to activate the configuration.</p> <p>When the progress meter disappears the configuration has been applied.</p> |

8. Management Server Procedures

8.1 IPM Management Server

This procedure configures and IPMs the DL360, DL380, or Oracle rack mount server.

Needed Material: TPD Initial Product Manufacture Software Installation Procedure, E53017.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 54. IPM the Management Server

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Configure and IPM the DL360, DL380, or Oracle RMS. | <p>Follow <i>TPD Initial Product Manufacture Software Installation Procedure</i>, E53017, sections 3.1 through 3.4 to configure and IPM the management server.</p> <p>For a DL360 G6/G7, DL380 G6/Gen8/Gen9, or Oracle server, the correct options to use for the IPM of the management server are:</p> <pre>TPDnoraaid console=tty0 diskconfig=HWRAID,force</pre> <p>Notes:</p> <ul style="list-style-type: none"> • If you are using a serial console for installation, do not use the <code>console=tty0</code> option. • Do not use the remote serial console for installation. |
| 2. <input type="checkbox"/> | Verify the initial product manufacture | Follow section 3.5 in <i>Initial Product Manufacture</i> , E53017, to verify the IPM completed successfully. |

8.2 Upgrade Management Server Firmware

If Oracle Consulting Services or any other Oracle Partner is providing services to a customer that includes installation and/or upgrade then, as long as the terms of the scope of those services include that Oracle Consulting Services is employed as an agent of the customer (including update of Firmware on customer provided services), then Oracle consulting services can install FW they obtain from the customer who is licensed for support from HP.

Note: This procedure uses a custom SPP version that cannot be obtained from the customer and, therefore, cannot be used for a Software Centric Customer. Software Centric Customers must ensure their firmware versions match those detailed in [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes.

8.2.1 Upgrade DL360/DL380 Server Firmware

This procedure upgrades the DL360 or DL380 server firmware.

The HP Support Pack for ProLiant installer automatically detects the firmware components available on the target server and only upgrades those components with firmware older than what is provided by the SPP in the HP FUP version being used.

Prerequisite: 8.1 IPM Management Server

Needed Material

- HP Service Pack for ProLiant (SPP) firmware ISO image
- HP MISC firmware ISO image (for errata updates if applicable)
- [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes
- USB Flash Drive (4GB or larger) if upgrading with USB media.

Note: For the **Update Firmware Errata** step, check [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes to see if there are any firmware errata items that apply to the server being upgraded. If there is, there is a directory matching the errata's ID in the **/errata** directory of the

HP MISC firmware ISO image. The errata directories contain the errata firmware and a README file detailing the installation steps.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

The minimum supported HP Solutions Firmware Upgrade Pack for Platform 7.6.x is release 2.2.12. However, when upgrading firmware, it is recommended that the latest release be used. Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes for important information on firmware upgrades and follow the procedures in the [2] HP Solutions Firmware Upgrade Pack, Upgrade Guide to upgrade the firmware.

8.2.2 Upgrade Oracle Rack Mount Server Firmware

This procedure updates firmware on Oracle RMS.

Needed Material

- Oracle Firmware Upgrade Pack 3.x.x Release Notes
- Oracle Firmware Upgrade Pack 3.x.x Upgrade Guide

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

The minimum supported Oracle Firmware Upgrade Pack for Platform 7.6.x is release 3.1.6. However, when upgrading firmware, it is recommended that the latest release be used. Refer to Oracle Firmware Upgrade Pack Release Notes for procedures on how to obtain the firmware, then follow the procedures in the Oracle Firmware Upgrade Pack Upgrade Guide to upgrade the firmware.

9. PMAC Procedures

Deploying a VM guest in the absence of a PMAC is complicated. To facilitate this, the PMAC media includes a guest archive and a script that deploys the running PMAC into a state where the Initialization process can begin. The general procedure is:

- Install TVOE 3.5 on the management server using the ILO.
- Create and configure the management bridge.
- Attach PMAC media to the TVOE (USB).
- Mount the media.
- Use the <mount-point>/upgrade/pmac-deploy script to create the VM and configure the guest on the first boot.
- Navigate browser to the management IP address of the deployed PMAC.
- Perform Initial Configuration.

Needed Material

Use the completed NAPD information to fill in the appropriate data in this procedure's reference tables. The following are provided to aid with the data collection for the TVOE management server and the PMAC application hosted on the Management Server TVOE.

- Determine if the network configuration of this management server is Non-Segregated or Segregated.

Note: The term **Segregated networks** refers to the separation of the Management server's control and plat-management networks into separate physical NICs.

- Determine the TVOE management server's required network interface, bond, and Ethernet device, and route data.
- Determine if the control network on the TVOE management server is to be tagged. If appropriate, fill in the <control VLAN ID> value in the table; otherwise, the control network is not tagged.

- Determine if the management network on the TVOE management Server is to be tagged. If appropriate, fill in the <management_VLAN_ID> value in the table; otherwise, the management network is not tagged.
- Determine the bridge name to be used on the TVOE management server for the management network. Fill in the <TVOE_Management_Bridge> value in the table.
- Determine if the NetBackup feature is enabled
 - Determine the NetBackup network on the TVOE management server is to be tagged. If appropriate, fill in the <NetBackup_VLAN_ID> value in the table; otherwise, the NetBackup network is not tagged.
 - Determine the bridge name to be used on the TVOE management server for the NetBackup network. Fill in the <TVOE_NetBackup_Bridge> value in the table.
 - Determine if the NetBackup network is to be configured with jumbo frames. If appropriate, fill in the <NetBackup_MTU_size> value in the table; otherwise, the NetBackup network uses the default MTU size.
 - If the PMAC NetBackup feature is enabled, and the backup service will be routed, with a source interface different from the management interface where the default route is applied, then define the route during PMAC initialization as a host route to the NetBackup server.
- The PMAC initialization profiles have been designed to configure the PMAC's networks and features. Profiles must identify interfaces. Existing profiles provided by PMAC use standard named interfaces (control, management). No VLAN tagging is expected on the PMAC's interfaces, all tagging should be handled on the TVOE management server configuration.

Procedure Reference Tables

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Fill in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

| Network Interface | DL360 (without HP NC364T 4pt Gb) | DL360 (with HP NC364T 4pt Gb in PCI Slot 2) | DL380 (with only LOM 4pt NICs) (G6) | DL380 (with HP 4pt Gb in PCI Slot 1) (Gen8, 9) | DL380 (with HP 4pt Gb in PCI Slot 3) (G6) | Oracle RMS (without 10GigE card) | | | DL380 (with HP 1Gb 4pt 331FLR Adapter) (Gen9) |
|------------------------|----------------------------------|---|-------------------------------------|--|---|----------------------------------|---------------|-------|---|
| | | | | | | X3-2 | X5-2 and X6-2 | X7-2 | |
| <ethernet_interface_1> | eth01 | eth01 | eth01 | eth01 | eth01 | eth01 | eth01 | eth02 | eth01 |
| <ethernet_interface_2> | eth02 | eth02 | eth02 | eth02 | eth02 | eth02 | eth03 | eth03 | eth02 |
| <ethernet_interface_3> | | eth21 | | eth11 | eth31 | eth03 | eth02 | eth21 | eth03 |
| <ethernet_interface_4> | | eth22 | | eth12 | eth32 | eth04 | eth04 | Eth23 | eth04 |
| <ethernet_interface_5> | | eth23 | | eth04 | eth04 | | | | eth05 |

| PMAC Interface Alias | TVOE Bridge Name | TVOE Bridge Interface |
|----------------------|-----------------------------------|--|
| control | control | <TVOE_Control_Bridge_Interface> _____ Default is bond0 |
| management | <TVOE_Management_Bridge> _____ | <TVOE_Management_Bridge_Interface> _____ |

| PMAC Interface Alias | TVOE Bridge Name | TVOE Bridge Interface |
|----------------------|----------------------------------|--|
| NetBackup | <TVOE_NetBackup_Bridge> _____ | <TVOE_NetBackup_Bridge_Interface> _____ |

| Variable and Description | Value |
|---|-------|
| <p><control_VLAN_ID> For non-segregated networks, the control network may have a VLAN ID assigned. In most cases, there is none.</p> | |
| <p><base_device_hosting_control_network> If <control_VLAN_ID> has a value, then the device used for the control network <TVOE_Control_Bridge_Interface> has a tagged interface name. The base device for the control network is the untagged interface name. For example, if the device interface is bond1.2 then the base device is bond1.</p> | |
| <p><management_VLAN_ID> For non-segregated networks, the management network is on a tagged VLAN coming in on bond0.</p> | |
| <p><mgmtVLAN_gateway_address> Gateway address used for routing on the management network.</p> | |
| <p><NetBackup_server_IP> The IP address of the remote NetBackup server.</p> | |
| <p><NetBackup_VLAN_ID> For non-segregated networks, the NetBackup network is on a tagged VLAN coming in on bond0.</p> | |
| <p><NetBackup_gateway_address> Gateway address used for routing on the NetBackup network.</p> | |
| <p><NetBackup_network_IP> The network IP for the NetBackup network.</p> | |
| <p><PMAC_NetBackup_netmask_or_prefix> The IPv4 netmask or IPv6 prefix assigned to the PMAC for participation in the NetBackup network.</p> | |
| <p><PMAC_NetBackup_IP_address> The IP address assigned to the PMAC for participation in the NetBackup network.</p> | |
| <p><NetBackup_MTU_size> If desired, the MTU size can be set to tune the NetBackup network traffic.</p> | |
| <p><management_server_mgmt_IP_address> The TVOE management server's IP address on the management network.</p> | |

| Variable and Description | Value |
|---|-------|
| <PMAC_mgmt_IP_address> The PMAC application's IP address on the management network. | |
| <mgmt_netmask_or_prefix> The IPv4 netmask or IPv6 prefix for the management network. | |
| <PMAC_control_IP_address> The PMAC application's IP address on the control network. | |
| <control_netmask> The IP netmask for the control network. | |

| Network Bond Interface | Enslaved Interface 1 | Enslaved Interface 2 |
|------------------------|------------------------------|--|
| bond0 | For segregated networks only | |
| bond1 | | |
| bond2 | | Bonding used for abstraction only, not multiple interfaces |

9.1 Install TVOE on the Management Server

Install the TVOE hypervisor platform on the management server. The PMAC is not available to do an IPM using TVOE on the management server. It is necessary to provide the TVOE media using a bootable USB drive.

Needed Material: TPD or TVOE installation media to be used for IPM.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

1. Configure the iLO IP address. For more information, refer to Appendix F in the [1] TPD Initial Product Manufacture Software Installation Procedure.
2. Configure and IPM the DLL360 or DL380 server by following 8.1 IPM Management Server.

For a DL360 G6/G7 or DL380 G6/Gen8/Gen9 server, the correct options to use for the IPM of the management server are:

```
TPDnoraaid console=tty0 diskconfig=HWRAID,force
```

Note: Do not use the remote serial console for installation.

9.2 Configure TVOE Network

This procedure configures the TVOE network.

Prerequisite: 9.1 Install TVOE on the Management Server

Note: The output shown in this procedure is for illustrative purposes only. The site information for the system determines the network interfaces (network devices, bonds, and bond-enslaved devices) to configure.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | TVOE Management Server iLO: Login | <ol style="list-style-type: none"> Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. <code>http://<management_server_iLO_IP></code> Click on the Remote Console tab and open the Integrated Remote Console on the server. Click Yes if the Security Alert displays. |
| 2. <input type="checkbox"/> | TVOE Management Server: Configure the control network bond for back to back configurations (optional) | <p>If the control network for the RMS servers consists of direct connections between the servers with no intervening switches (known as a back-to-back configuration), execute this step to set the primary interface of bond0 to <ethernet_interface_1>; otherwise, skip to the next step.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --device=bond0 --onboot=yes --type=Bonding --mode=active-backup --miimon=100 --primary=<ethernet_interface_1>Interface bond0 updated</pre> |
| 3. <input type="checkbox"/> | TVOE Management Server: Verify the control network bridge | <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=control Bridge Name: control On Boot: yes Protocol: dhcp Persistent: yes Promiscuous: no Hwaddr: 00:24:81:fb:29:52 MTU: Bridge Interface: bond0</pre> <p>If the bridge has been configured, skip to the next step.</p> |
| 4. <input type="checkbox"/> | TVOE iLO: Create a tagged control interface and bridge (optional) | <p>If you are using a tagged control network interface on this PMAC, then complete this step using values for the control interface on bond0 from the preceding tables; otherwise, proceed to the next step.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --delBridgeInt=bond0 Interface bond0 updated Bridge control updated \$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_Control_Bridge_Interface> --onboot=yes Interface <TVOE_Control_Bridge_Interface> created \$ sudo /usr/TKLC/plat/bin/netAdm set --type=Bridge --name=control --bridgeInterfaces=<TVOE_Control_Bridge_Interface></pre> |

Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|-----------------|---|---|
| <p>5. □</p> | <p>TVOE Management Server: Verify the non-segregated management network</p> | <p>This step only applies if the management network is tagged (non-segregated). This example shows the management bridge configured on a non-segregated network setup.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --device=bond0.2 Protocol: none On Boot: yes IP Address: Netmask: Bridge: Member of bridge management</pre> <p>If the device has been configured, skip to the next step.</p> <p>This example shows a PMAC management server configuration in a non-segregated network, untagged control network, and a tagged management network.</p> <p>Create a tagged device for the management device.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add -- device=<TVOE_Management_Bridge_Interface> --onboot=yes Interface <TVOE_Management_Bridge_Interface> added</pre> |
| <p>6. □</p> | <p>TVOE Management Server: Verify the untagged/segregated management network</p> | <p>This step only applies if the management network is untagged (segregated). This example shows the management bridge configured on a segregated network setup.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query -- device=<TVOE_Management_Bridge_Interface> Protocol: none On Boot: yes IP Address: Netmask: Bonded Mode: active-backup Enslaving: <ethernet_interface_3> <ethernet_interface_4></pre> <p>If the bridge has been configured, skip to the next step.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add -- device=<TVOE_Management_Bridge_Interface> --onboot=yes -- type=Bonding --mode=active-backup --miimon=100 -- bondInterfaces="<ethernet_interface_3>,<ethernet_interface_4> Interface <TVOE_Management_Bridge_Interface> added</pre> |

Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|-----------------|--|--|
| <p>7. □</p> | <p>TVOE Management Server: Verify the management bridge</p> | <p>This example shows the management bridge configured on a non-segregated network setup.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=management Bridge Name: management On Boot: yes Protocol: none IP Address: 10.240.4.86 Netmask: 255.255.255.0 Promiscuous: no Hwaddr: 00:24:81:fb:29:52 MTU: Bridge Interface: bond0.2</pre> <p>If the bridge has been configured, skip to the next step. For this example, create a tagged device for the management device.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_Management_Bridge> --address=<management_server_mgmt_ip_address> --netmask=<mgmt_netmask_or_prefix> --onboot=yes --bridgeInterfaces=<TVOE_Management_Bridge_Interface></pre> |

Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|-----------------|---|---|
| <p>8. □</p> | <p>TVOE Management Server: Verify the NetBackup network, if needed</p> | <p>If the NetBackup feature is not needed, skip to the next step.</p> <p>This example shows the NetBackup bridge is configured.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --type=Bridge --name=netbackup</pre> <pre>Bridge Name: netbackup On Boot: yes Protocol: none IP Address: 10.240.6.2 Netmask: 255.255.255.0 Promiscuous: no Hwaddr: 00:24:81:fb:29:58 MTU: Bridge Interface: bond2</pre> <p>If the bridge has been configured, skip to the next step.</p> <p>This example shows a TVOE management server configuration with the NetBackup feature enabled. The NetBackup network is configured with a non-default MTU size. The MTU size must be consistent between a network bridge, device, or bond, and associated VLANs.</p> <p>Select only one of the following configurations:</p> <p>Option 1: Create NetBackup bridge using an untagged native interface.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --bootproto=none --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<Ethernet_interface_5> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix></pre> <p>Option 2: Create NetBackup bridge using a tagged device.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --device=<TVOE_NetBackup_Bridge_Interface> --onboot=yes Interface <TVOE_NetBackup_Bridge_Interface> added \$ sudo /usr/TKLC/plat/bin/netAdm add --type=Bridge --name=<TVOE_NetBackup_Bridge> --onboot=yes --MTU=<NetBackup_MTU_size> --bridgeInterfaces=<TVOE_NetBackup_Bridge_Interface> --address=<TVOE_NetBackup_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix></pre> |


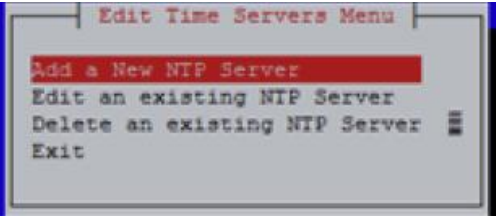
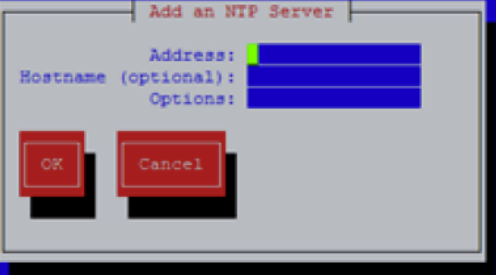
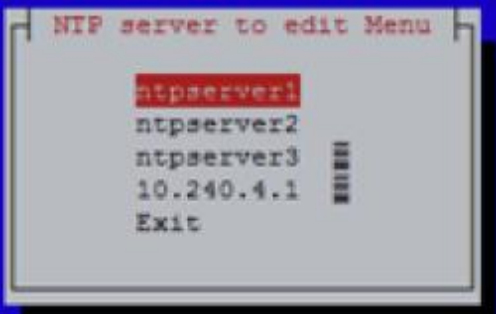
Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|---|--|---|
| <p>9. <input type="checkbox"/></p> | <p>TVOE Management Server: Set up syscheck</p> | <p>syscheck must be configured to monitor bond interfaces. Replace bondedInterfaces with bond0 or bond0,bond1, if segregated networks are used:</p> <pre>\$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=<bondedInterfaces> \$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable \$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond</pre> <p>This example shows the setup of syscheck with a single bond, bond0:</p> <pre>\$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=bond0 \$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable \$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond</pre> <p>This example shows the setup of syscheck with multiple bonds, bond0 and bond1:</p> <pre>\$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond --set --var=DEVICES --val=bond0,bond1 \$ sudo /usr/TKLC/plat/bin/syscheckAdm net ipbond -enable \$ sudo /usr/TKLC/plat/bin/syscheck -v net ipbond</pre> |
| <p>10. <input type="checkbox"/></p> | <p>TVOE Management Server: Verify the default route</p> | <p>This example shows the default route on the management bridge is configured.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --route=default --device=management Routes for TABLE: main and DEVICE: management * NETWORK: default GATEWAY: 10.240.4.1</pre> <p>If the route has been configured, skip to the next step.</p> <p>This example adds the default route on a management network.</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=default --device=<TVOE_Management_Bridge> --gateway=<mgmt_gateway_address> Route to <TVOE_Management_Bridge> added</pre> |

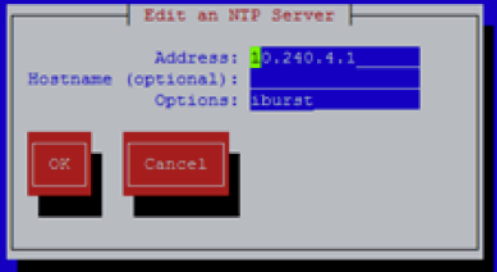
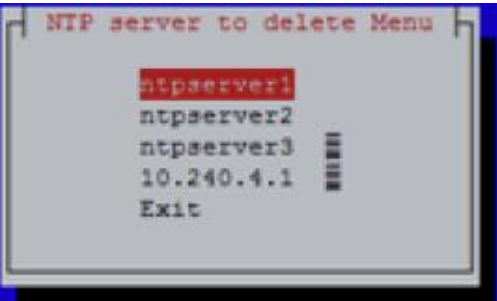
Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|---|---|---|
| <p>11. <input type="checkbox"/></p> | <p>TVOE Management Server: Verify the NetBackup route (optional)</p> | <p>If the NetBackup network is a unique network for NetBackup data, verify the existence of the appropriate NetBackup route. This example shows the route on the NetBackup bridge is configured. If the NetBackup route is to be a network route, then: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --route=net --device=<TVOE_NetBackup_Bridge></pre> <p>Routes for TABLE: main and DEVICE: netbackup * NETWORK: net GATEWAY: 169.254.253.1</p> <p>If the NetBackup route is to be a host route then: <pre>\$ sudo /usr/TKLC/plat/bin/netAdm query --route=host --device=<TVOE_NetBackup_Bridge></pre> <p>Routes for TABLE: main and DEVICE: netbackup * NETWORK: host GATEWAY: 169.254.253.1</p> <p>If the route has been configured, skip to the next step. This example adds network route on management network. <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net --device=<TVOE_Management_Bridge> --gateway=<NetBackup_gateway_address> --address=<NetBackup_network_IP> --netmask=<TVOE_NetBackup_Netmask_or_prefix></pre> <p>Route to <TVOE_NetBackup_Bridge> added</p> <p>This example adds a host route on management network. Note: For the configuration of a host route, the <TVOE_NetBackup_Netmask> is set to 255.255.255.255. <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=host --device=<TVOE_Management_Bridge> --gateway=<NetBackup_Server_IP> --address=<NetBackup_Server_IP></pre> <p>Route to <TVOE_NetBackup_Bridge> added</p> </p></p></p></p> |
| <p>12. <input type="checkbox"/></p> | <p>TVOE Management Server: Set hostname</p> | <pre>\$ sudo /bin/su - platcfg</pre> <ol style="list-style-type: none"> 1. Navigate to Server Configuration > Hostname and set the hostname. 2. Set TVOE Management Server hostname 3. Click OK. 4. Navigate out of Hostname |
| <p>13. <input type="checkbox"/></p> | <p>TVOE Management Server: Set time zone and/or hardware clock</p> | <ol style="list-style-type: none"> 1. Navigate to Server Configuration > Time Zone. 2. Click Edit. 3. Set the time zone and/or hardware clock to GMT (Greenwich Mean Time). 4. Click OK. 5. Navigate out of Server Configuration. |
| <p>14. <input type="checkbox"/></p> | <p>TVOE Management</p> | <p>Three or more NTP sources are required.</p> <ol style="list-style-type: none"> 1. Login as the platcfg user on the server. |


Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|------|---|--|
| | <p>Server: Configure NTP servers for a server based on TPD</p> | <p>2. Navigate to Network Configuration > NTP.</p>  <pre>Platform Configuration Utility 3.08 (C) 2003 - 2013 Tekelec, Inc. Hostname: pmac033-1 Time Servers NTP Servers Address: Hostname: Options: ----- - 10.240.4.90 ntpserver1 iburst dynamic iburst ntpserver2 iburst dynamic iburst ntpserver3 iburst dynamic iburst</pre> <p>3. Click Edit.</p> <p>4. Click Add a New NTP Server.</p>  <pre>Edit Time Servers Menu Add a New NTP Server Edit an existing NTP Server Delete an existing NTP Server Exit</pre> <p>5. Type the appropriate data and click OK.</p>  <pre>Add an NTP Server Address: Hostname (optional): Options: OK Cancel</pre> <p>The default NTP option is iburst. Additional NTP options are listed on the ntp.conf man page, some of the valid options are burst, minpoll, and maxpoll.</p> <p>6. Click Edit an existing NTP Server.</p>  <pre>NTP server to edit Menu ntpserver1 ntpserver2 ntpserver3 10.240.4.1 Exit</pre> |

Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|---|--|--|
| | | <p>7. Select the NTP server and edit information as needed.</p>  <p>8. If deleting an existing NTP server, select Delete an existing NTP Server.</p>  <p>9. Select the NTP server and press Enter.</p> <p>10. Click Yes to confirm deleting the NTP server.</p> <p>11. Restart the NTP server.</p> <p>12. Click Exit on each menu until platcfg exits.</p> |
| <p>15. <input type="checkbox"/></p> | <p>TVOE Management Server: Set SNMP trap destination to a server based on TPD</p> | <p>All alarm information is sent to the NMS located at the destination. Follow 12.3 Add SNMP Trap Destination on TPD-Based Application. Note: If NetBackup is to be configured, execute 3.2.1 Configure Cisco 4948/4948E/4948E-F Aggregation Switches (PMAC Installed) (netConfig) and then execute 13.2 Configure TVOE NetBackup Client on the TVOE host.</p> |
| <p>16. <input type="checkbox"/></p> | <p>TVOE Management Server: Verify server health</p> | <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> <p>Alarms may display if network connectivity has not been established.</p> |
| <p>17. <input type="checkbox"/></p> | <p>TVOE Management Server: Set time based on NTP server</p> | <pre>\$ sudo /sbin/service ntpd stop \$ sudo /usr/sbin/ntpdate ntpserver1 \$ sudo /sbin/service ntpd start</pre> <p>Reboot the server.</p> <pre>\$ sudo /sbin/init 6</pre> |

Procedure 55. Configure the TVOE Network

| Step | Procedure | Results |
|------------------|---|---|
| <p>18. □</p> | <p>TVOE Management Server: Back up system files to use when restoring a system</p> | <p>Note: The backup image is to be transferred to a customer device.</p> <ol style="list-style-type: none"> 1. Login as the platcfg user on the server. 2. Navigate to Maintenance > Backup and Restore. 3. Click Backup Platform (CD/DVD).  <p>Note: If this operation is attempted on a system without media (for example, the CD/DVD), a No disk device available. This is normal on systems without a CD ROM device message displays. Ignore the message and press any key to continue.</p> <ol style="list-style-type: none"> 4. Click Build ISO file only. The Creating ISO Image. . . message may display. After the ISO is created, platcfg returns to the Backup TekServer Menu screen. The ISO has now been created and is located in the /var/TKLC/bkp/ directory. An example filename of a backup file created is hostname1307466752-plat-app-201104171705.iso. 5. Click Exit on each menu until platcfg exits. The SSH connection to the TVOE server terminates. 6. Log into the customer server and copy the backup image to the customer server where it can be safely stored. <p>Note: This step assumes the network configuration is complete and the source and target servers can connect to each other. If this is not the case, skip this step for now and return to it when the network configuration is complete.</p> <p>If the customer system is a Linux system, execute the following command to copy the backup image to the customer system.</p> <pre># scp tvoexfer@<TVOE IP Address>:/var/TKLC/bkp/* /path/to/destination/</pre> <p>When prompted, enter the tvoexfer user password and press Enter.</p> <pre># scp tvoexfer@<TVOE IP Address>:/var/TKLC/bkp/* /path/to/destination/ tvoexfer@10.24.34.73's password: hostname1301859532-plat-app-301104171705.iso 100% 134MB 26.9MB/s 00:05</pre> <p>If the customer system is a Windows system, refer to Appendix A Using WinSCP to copy the backup image to the customer system.</p> |

9.3 Deploy PMAC Guest

The pmac-deploy script deploys a PMAC guest in the absence of a PMAC to create the guest and install the OS and application. This is done at build time and the system disk image is kept on the PMAC media, along with this script. The media is either physical media (USB) or a disk image (.iso file) from OSDC. The media can be stored on a USB and mounted. It can be downloaded to the TVOE (usually /var/TKLC/upgrade), but that is recommended only for lab deployments and depends on the storage available on the TVOE host. Once the PMAC media is mounted, the pmac-deploy script can be found in the upgrade directory of the media.

Prerequisites:

- 9.1 Install TVOE on the Management Server
- 9.2 Configure TVOE Network
- PMAC Installation Media

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 56. Deploy PMAC Guest

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | TVOE Management Server iLO: Login | 1. Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. <code>http://<management_server_iLO_IP></code> 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click Yes if the Security Alert displays. Note: Alternatively, you can log into the management console through PuTTY. Connect to the server using <code><management_server_iLO_IP></code> Start the virtual serial port by executing the <code>vsp</code> command. Log into the remote server using <code>admusr</code> credentials. |
| 2. <input type="checkbox"/> | TVOE Management Server: Mount the PMAC media | <pre>\$ sudo /bin/ls /media/*/*.iso /media/usb/872-2441-104-5.0.0_50.8.0-PMAC-x86_64.iso \$ sudo /bin/mount -o loop /media/usb/872-2441-104-5.0.0_50.8.0-PMACx86_64.iso /mnt/upgrade</pre> |

Procedure 56. Deploy PMAC Guest

| Step | Procedure | Results |
|--|---|--|
| <p>3. <input type="checkbox"/></p> | <p>TVOE Management Server: Validate the PMAC media</p> | <p>Execute the self-validating media script:</p> <pre> \$ cd /mnt/upgrade/upgrade \$ sudo .validate/validate_cd Validating cdrom... UMVT Validate Utility v2.2.2, (c)Tekelec, June 2012 Validating <device or ISO> Date&Time: 2012-10-25 10:07:01 Volume ID: tklc_872-2441-106_Rev_A_50.11.0 Part Number: 872-2441-106_Rev_A Version: 50.11.0 Disc Label: PMAC Disc description: PMAC The media validation is complete, the result is: PASS CDROM is Valid </pre> <p>If the media validation fails, the media is not valid and should not be used.</p> |

Procedure 56. Deploy PMAC Guest

| Step | Procedure | Results |
|-----------------|--|---|
| <p>4. □</p> | <p>TVOE Management Server: Deploy PMAC instance</p> | <p>Using the pmac-deploy script, deploy the PMAC instance using the configuration detailed by the completed NAPD.</p> <p>For this example, a PMAC is deployed without NetBackup.</p> <pre>\$ cd /mnt/upgrade/upgrade \$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name> --controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask_or_prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<TVOE_Management_server_ip_address></pre> <p>Deploying a PMAC with the NetBackup feature requires the --netbackupVol option, which creates a separate NetBackup logical volume on the TVOE host of PMAC. If the NetBackup feature's source interface is different from the management interface, include the --bridge and --nic as shown in this example.</p> <pre>\$ cd /mnt/upgrade/upgrade \$ sudo ./pmac-deploy --guest=<PMAC_Name> --hostname=<PMAC_Name> --controlBridge=<TVOE_Control_Bridge> --controlIP=<PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask_or_prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<TVOE_Management_server_ip_address> --netbackupVol --bridge=<TVOE_NetBackup_Bridge> --nic=netbackup --isoimagesVolSizeGB=20</pre> <p>Note: The NUMA settings can be configured using new options added to the pmac-deploy command. Please see section Configuring NUMA on pmac-deploy for instructions on using the new options.</p> <p>Note: If a mistake in the pmac-deploy is identified during this step the operator under the advisement of customer service can remove the guest with the following command:</p> <pre>\$ sudo /usr/TKLC/plat/bin/guestMgr --remove <PMAC_Name></pre> |

Procedure 56. Deploy PMAC Guest

| Step | Procedure | Results |
|--------------------------------|--|---|
| 5. <input type="checkbox"/> | TVOE Management Server: Unmount the media and remove | After the PMAC deploys and boots, the management and control network comes up. At that point unmount the media and remove the PMAC media. <pre>\$ cd / \$ sudo /bin/unmount /mmmnt/upgrade</pre> |

9.4 Set Up PMAC

This procedure configures the PMAC application environment on the management server TVOE host; and initializes the PMAC application. When this procedure is complete, the PMAC application environment is configured to allow configuration of system network assets associated with the management server.

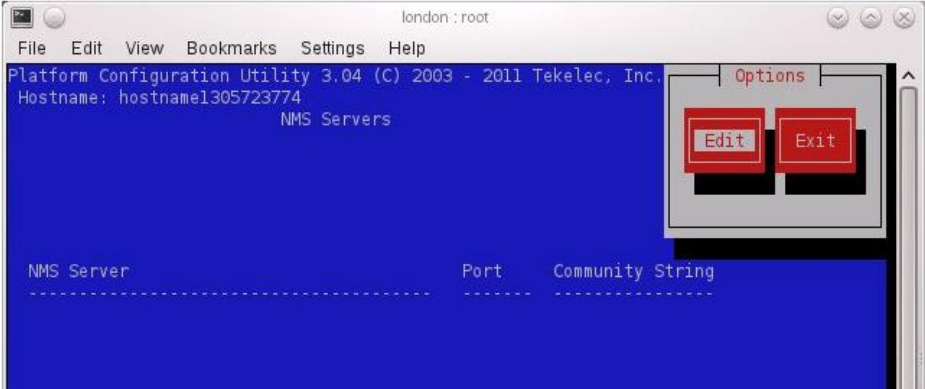
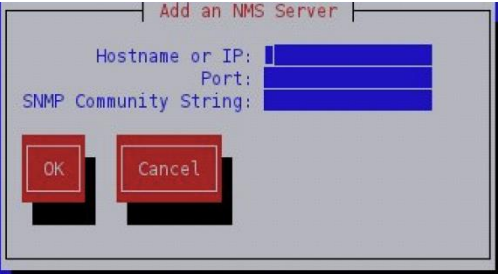
Prerequisite: 9.3 Deploy PMAC Guest

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

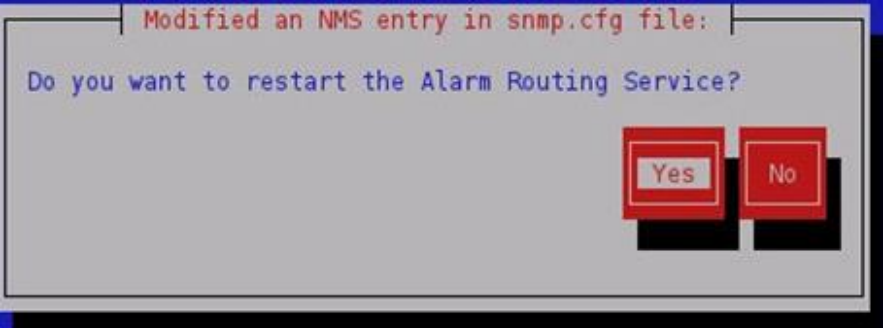
Procedure 57. Set Up PMAC

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | TVOE Management Server iLO: Login | <ol style="list-style-type: none"> Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. <code>http://<management_server_iLO_IP></code> Click on the Remote Console tab and open the Integrated Remote Console on the server. Click Yes if the Security Alert displays. |
| 2. <input type="checkbox"/> | TVOE Management Server iLO: Login | <p>Log into PMAC with admusr credentials.</p> <p>Note: On a TVOE host, if you open the virsh console, for example, <code>\$ sudo /usr/bin/virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or the output is not correct, then there is likely a stuck virsh console command already being run on the TVOE host. Exit out of the virsh console, run <code>ps -ef grep virsh</code>, and then kill the existing process <code>kill -9 <PID></code>. Then execute the <code>virsh console X</code> command. Your console session should now run as expected.</p> <p>Login using virsh and wait until you see the login prompt. If a login prompt does not appear after the guest is finished booting, press Enter to make one appear:</p> <pre> \$ sudo /usr/bin/virsh virsh # list Id _Name _ _ _ _ _ State 4 pmacU17-1 running virsh # console pmacU17-1 [Output Removed] ##### 1371236760: Upstart Job readahead-collector: stopping 1371236767: Upstart Job readahead-collector: stopped ##### CentOS release 7.5 (Final) Kernel 2.6.32-358.6.1.el6prere16.5.0_82.16.0.x86_64 on an x86_64 pmacU17-1 login: </pre> |

Procedure 57. Set Up PMAC

| Step | Procedure | Results |
|--|--|--|
| <p>3. <input type="checkbox"/></p> | <p>TVOE Management Server iLO: Verify PMAC configure correctly</p> | <p>Run the following command (there should be no output):</p> <pre>\$ sudo /bin/ls /usr/TKLC/plat/etc/deployment.d/</pre> |
| <p>4. <input type="checkbox"/></p> | <p>TVOE Management Server iLO: Determine and set the time zone</p> | <p>Valid time zones can be found on the server in the /usr/share/zoneinfo directory. Only time zones within the sub-directories (for example, America, Africa, Pacific, Mexico, etc.) are valid with platcfg.</p> <p>To set the time zone, run:</p> <pre>\$ sudo /usr/TKLC/smac/bin/set_pmac_tz.pl <timezone></pre> <p>For Example:</p> <pre>\$ sudo set_pmac_tz.pl America/New_York</pre> <p>Verify the time zone has been updated by running:</p> <pre>\$ sudo /bin/date</pre> |
| <p>5. <input type="checkbox"/></p> | <p>TVOE Management Server: Set SNMP trap destination to a server based on TPD</p> | <p>All alarm information is sent to the NMS located at the destination.</p> <ol style="list-style-type: none"> 1. Login as the platcfg user on the server. 2. Navigate to the NMS Server Configuration screen. 3. Navigate to Network Configuration > SNMP Configuration > NMS Configuration.  <ol style="list-style-type: none"> 4. Click Edit. 5. Click Add a New NMS Server. 6. Type the appropriate data and click OK.  |

Procedure 57. Set Up PMAC

| Step | Procedure | Results |
|------------------------------------|--|---|
| | | <p>7. Click Exit and Yes.</p>  <p>8. Click Exit on each menu until platcfg exits.</p> |
| <p>6. <input type="checkbox"/></p> | <p>TVOE Management Server iLO: Login</p> | <p>Log into the PMAC as the admusr user.</p> |
| <p>7. <input type="checkbox"/></p> | <p>TVOE Management Server iLO: Reboot</p> | <p>Reboot the server to ensure all processes are started with the new time zone.</p> <pre>\$ sudo /sbin/init 6</pre> |
| <p>8. <input type="checkbox"/></p> | <p>PMAC (optional)</p> | <p>Gather and prepare configuration files that must be located on the PMAC. These may be required to proceed with the application installation after the PMAC has been deployed, but before it has been initialized. These files are usually located within a given ISO on the physical media.</p> <p>Note: This is an optional step only required if needed by an application.</p> <p>Needed Material</p> <ul style="list-style-type: none"> • HP Misc. Firmware DVD • [2] HP Solutions Firmware Upgrade Pack <ol style="list-style-type: none"> 1. Once the PMAC has completed rebooting, but before initializing, log into the PMAC as admusr using virsh on the management server iLO. 2. Create any necessary destination subdirectories in the PMAC /usr/TKLC/smac/etc directory, if not using an existing directory to transfer files. For each subdirectory created, set the directory's ownership. If you create multiple levels of subdirectories, set the ownership of each level separately. <pre>\$ sudo mkdir /usr/TKLC/smac/etc/<dir1> \$ sudo chown pmacd:pmacbackup /usr/TKLC/smac/etc/<dir1> \$ sudo mkdir /usr/TKLC/smac/etc/<dir1>/<dir2> \$ sudo chown pmacd:pmacbackup /usr/TKLC/smac/etc/<dir1>/<dir2></pre> 3. Make the media available to the TVOE host server. Mount the media on the TVOE host using the following method: <ol style="list-style-type: none"> a. Insert the USB into an available USB slot on the TVOE host server and execute the following command to determine its location and the |

Procedure 57. Set Up PMAC

| Step | Procedure | Results |
|------------------------------------|--|---|
| | | <p>ISO to be mounted:</p> <pre>\$ sudo /bin/ls /media/*/*.iso</pre> <p>Example:</p> <pre>/media/sdd1/872-xxxx-104-5.0.0_50.8.0-application-x86_64.iso</pre> <p>Note: The USB device is added to the list of media devices once it is inserted into a USB slot on the TVOE host server.</p> <p>b. Note the device directory name under the media directory. This could be sdb1, sdc1, sdd1, or sde1, depending on the USB slot into which the media was inserted.</p> <p>c. Loop mount the ISO to the standard TVOE host mount point (if it is not already in use):</p> <pre>\$ sudo /bin/mount -o loop /media/<device directory>/<ISO Name>.iso /mnt/upgrade</pre> <p>4. Execute the following commands on the PMAC guest to copy the required files from the TVOE host to the PMAC guest. Wildcards can be used as necessary.</p> <pre>\$ sudo /usr/bin/scp -r admusr@<TVOE_management_ip_address>:/mnt/upgrade/<path to files>/* /<path to destination directory></pre> <p>5. Remove the application media from the TVOE host:</p> <pre>\$ sudo /bin/umount /mnt/upgrade</pre> |
| <p>9. <input type="checkbox"/></p> | <p>PMAC Application: Initialize</p> | <p>If performing the setup on a redundant PMAC, do not initialize, skip this step, and continue with step 12.</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</pre> <pre>1: Initialize PMAC COMPLETE - PMAC initialized</pre> <pre>Step 2: of 2 Started: 2012-07-13 08:23:55 running: 29</pre> <pre>sinceUpdate: 47</pre> <pre>taskRecordNum: 2 Server Identity:</pre> <pre>Physical Blade Location:</pre> <pre>Blade Enclosure:</pre> <pre>Blade Enclosure Bay:</pre> <pre>Guest VM Location:</pre> <pre>Host IP:</pre> <pre>Guest Name:</pre> <pre>TPD IP:</pre> <pre>Rack Mount Server:</pre> <pre>IP:</pre> <pre>Name:</pre> <p>The command displays IN_PROGRESS for a short time. Run the command until a COMPLETE or FAILED response displays.</p> |

Procedure 57. Set Up PMAC

| Step | Procedure | Results |
|---|--|--|
| <p>10. <input type="checkbox"/></p> | <p>PMAC: Perform a system health check</p> | <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> <p>This command should return no output on a healthy system.</p> <p>Note: An NTP alarm is detected if the system switches are not configured. Additionally, a tpdDefaultRouteNetworkError alarm may be detected if the system switches are not configured.</p> <pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre> <p>All processes should be running, displaying output similar to the following:</p> <pre>PMAC_Sentry_Status sentryd started: Mon Jul 23 17:50:49 2012 Current activity mode: ACTIVE Process ----- PID Status StartTS NumR smacTalk 9039 running Tue Jul 24 12:50:29 2012 2 smacMon 9094 running Tue Jul 24 12:50:29 2012 2 hpiPortAudit 9137 running Tue Jul 24 12:50:29 2012 2 snmpEventHandler 9176 running Tue Jul 24 12:50:29 2012 2 Fri Aug 3 13:16:35 2012 Command Complete.</pre> |
| <p>11. <input type="checkbox"/></p> | <p>PMAC Application: Verify release</p> | <p>Verify the PMAC application product release is as expected.</p> <p>Note: If the PMAC application product release is not as expected, STOP and contact Error! Bookmark not defined.</p> <pre>\$ sudo /usr/TKLC/plat/bin/appRev Install Time: Mon Mar 14 16:12:33 2016 Product Name: PMAC Product Release: 6.2.0.0.0_62.16.0 Base Distro Product: TPD Base Distro Release: 7.2.0.0.0_88.17.0 Base Distro ISO: TPD.install-7.2.0.0.0_88.17.0-OracleLinux6.7-x86_64.iso ISO name: PMACBLD-6.2.0.0.0_62.16.0.iso OS: OracleLinux 6.7</pre> |
| <p>12. <input type="checkbox"/></p> | <p>Virsh Console: Log out</p> | <p>Exit the virsh console session using Appendix E.2 Exit a Guest Console Session on an iLO.</p> |
| <p>13. <input type="checkbox"/></p> | <p>Management Server iLO: Exit the TVOE console</p> | <pre>\$ logout</pre> <p>Close the iLO browser screen.</p> |
| <p>14. <input type="checkbox"/></p> | <p>Management Server iLO</p> | <p>If NetBackup needs to be configured on this PMAC, execute 9.22.2 Initialize PMAC Application Using the GUI and enable NetBackup.</p> |

9.5 Configure PMAC Application

Configuration of the PMAC application is typically performed using the PMAC GUI. This procedure defines application and network resources. At a minimum, you should define network routes and DHCP pools. Unlike initialization, configuration is incremental, so you may execute this procedure to modify the PMAC configuration.


Prerequisites:

- PMAC has been deployed and initialized, but possibly not fully configured.
- Aggregation switches have been properly configured.

Note: The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 58. Configure PMAC Application

| Step | Procedure | Results |
|--|---|---|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  <p>Navigate to Administration > PMAC Configuration.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUID: Select a profile</p> | <p>Click Feature Configuration.</p> |

Procedure 58. Configure PMAC Application

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|---|-------------------------------------|-------------|------|---------|------------------------|-----------------------------------|------------|--------------------------|------------|-----------------------|------------|-------------------------------------|--------------|----------------------------------|------------|--------------------------|--------------------|--------------------------|------------|-------------------------------------|----------------|------------------|------------|--------------------------|------------------------|---|------|--------------------------|
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUID: Configure optional features</p> | <p>If NetBackup is to be used, enable the NetBackup feature; otherwise, use the selected features as is. This image is for reference only.</p> <table border="1" data-bbox="513 363 1432 730"> <thead> <tr> <th>Feature</th> <th>Description</th> <th>Role</th> <th>Enabled</th> </tr> </thead> <tbody> <tr> <td>DEVICE.NETWORK.NETBOOT</td> <td>Network device PXE initialization</td> <td>Management</td> <td><input type="checkbox"/></td> </tr> <tr> <td>DEVICE.NTP</td> <td>PM&C as a time server</td> <td>Management</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PMAC.MANAGED</td> <td>Remote management of PM&C server</td> <td>Management</td> <td><input type="checkbox"/></td> </tr> <tr> <td>PMAC.REMOTE.BACKUP</td> <td>Remote server for backup</td> <td>Management</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PMAC.NETBACKUP</td> <td>NetBackup client</td> <td>Management</td> <td><input type="checkbox"/></td> </tr> <tr> <td>PMAC.IPV6.NOAUTOCONFIG</td> <td>PMAC IPv6 interface disable autoconfiguration</td> <td>NULL</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> <p style="text-align: center;"><input type="button" value="Add Role"/></p> <p>The Enabled checkbox selects the desired features. The Role field provides a list of known network roles with which the feature may be associated. The Description may be edited if desired.</p> <p>If the feature should be applied to a new network role (e.g., NetBackup), click Add Role. Enter the name of the new role and click Add.</p> <p>Note: Role names are not significant, they are only used to associate features with networks.</p> <p>The new role name displays in the Role list for features.</p> <p>When done, click Apply. This foreground task takes a few moments, and then refreshes the view with an Info or Error notice to verify the action. To discard changes, navigate away from the view.</p> | Feature | Description | Role | Enabled | DEVICE.NETWORK.NETBOOT | Network device PXE initialization | Management | <input type="checkbox"/> | DEVICE.NTP | PM&C as a time server | Management | <input checked="" type="checkbox"/> | PMAC.MANAGED | Remote management of PM&C server | Management | <input type="checkbox"/> | PMAC.REMOTE.BACKUP | Remote server for backup | Management | <input checked="" type="checkbox"/> | PMAC.NETBACKUP | NetBackup client | Management | <input type="checkbox"/> | PMAC.IPV6.NOAUTOCONFIG | PMAC IPv6 interface disable autoconfiguration | NULL | <input type="checkbox"/> |
| Feature | Description | Role | Enabled | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DEVICE.NETWORK.NETBOOT | Network device PXE initialization | Management | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DEVICE.NTP | PM&C as a time server | Management | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.MANAGED | Remote management of PM&C server | Management | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.REMOTE.BACKUP | Remote server for backup | Management | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.NETBACKUP | NetBackup client | Management | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.IPV6.NOAUTOCONFIG | PMAC IPv6 interface disable autoconfiguration | NULL | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 58. Configure PMAC Application

| Step | Procedure | Results |
|--|---|---|
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Reconfigure PMAC networks</p> | <p>Note: The network reconfiguration enters a tracked state. After you click Reconfigure, click Cancel to abort.</p> <ol style="list-style-type: none"> 1. Click Network Configuration and follow the wizard through the configuration task. 2. Click Reconfigure to display the network view. The default management and control networks should be configured correctly. Networks may be added, deleted, or modified from this view. They are defined with IPv4 dotted-quad address and netmasks, or with IPv6 colon hex address and a prefix. When complete, click Next. 3. Click Network Roles to change the role of a network. Network associations can be added (for example, NetBackup) or deleted. You cannot add a new role since roles are driven from features. When complete, click Next. 4. Click Network Interfaces to add or delete interfaces, and change the IP address within the defined network space. If you add a network (for example, NetBackup), the Add Interface view displays when you click Add. This view provides an editable list of known interfaces. You may add a new device here if necessary. The Address must be an IPv4 or IPv6 host address in the network. When complete, click Next. 5. Click Routes to add or delete route destinations. The initial PMAC deployment does not define routes. Most likely, you want to add a default route — the route already exists, but this action defines it to PMAC so it may be displayed by PMAC. Click Add. The Add Route view provides an editable list of known devices. Select the egress device for the route. Enter an IPv4 dotted-quad address and netmask or an IPv6 colon hex address and prefix for the route destination and next-hop gateway. Click Add Route. When complete, click Next. 6. Click DHCP Ranges to define DHCP pools used by servers that PMAC manages. Click Add. Enter the starting and ending IPv4 address for the range on the network used to control servers (by default, the control network). Click Add DHCP Range. Only one range per network may be defined. When all pools are defined, click Next. 7. Click Configuration Summary for a view of your reconfigured PMAC. Click Finish to open the background task that reconfigures the PMAC application. A Task and Info or Error notice displays to verify your action. 8. Verify your reconfiguration task completes. Navigate to Task Monitoring. As the network reconfigures, you have a brief network interruption. From the Background Task Monitoring view, verify the Reconfigure PMAC task succeeds. |
| <p>5. <input type="checkbox"/></p> | <p>PMAC GUI: Set site settings</p> | <p>Navigate to Administration > GUI Site Settings. Set the Site Name to a descriptive name, set the Welcome Message to display when logging in.</p> |

Procedure 58. Configure PMAC Application

| Step | Procedure | Results |
|--|--|---|
| <p>6. <input type="checkbox"/></p> | <p>PMAC: Application backup</p> | <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm backup</pre> <p>PMAC backup has been successfully initiated as task ID 7</p> <p>Note: The backup runs as a background task. To check the status of the background task use the PMAC GUI Task Monitor screen, or issue the command <code>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks</code>. The result should eventually be PMAC Backup successful and the background task should indicate COMPLETE.</p> <p>Note: The pmacadm backup command uses a naming convention that includes a date/time stamp in the filename (for example, backupPmac_20111025_100251.pef). In the example provided, the backup filename indicates it was created on 10/25/2011 at 10:02:51 am server time.</p> |
| <p>7. <input type="checkbox"/></p> | <p>PMAC: Verify backup was successful</p> | <p>Note: If the background task shows the backup failed, then the backup did not complete successfully. STOP and contact Error! Bookmark not defined.</p> <p>The output of <code>pmaccli getBgTasks</code> should look similar to the example below:</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks 2: Backup PMAC COMPLETE - PMAC Backup successful Step 2: of 2 Started: 2012-07-05 16:53:10 running: 4 sinceUpdate: 2 taskRecordNum: 2 Server Identity: Physical Blade Location: Blade Enclosure: Blade Enclosure Bay: Guest VM Location: Host IP: Guest Name: TPD IP: Rack Mount Server: IP: Name: ::</pre> |
| <p>8. <input type="checkbox"/></p> | <p>PMAC: Save the backup</p> | <p>The PMAC backup must be moved to a remote server. Transfer (sftp, scp, rsync, or preferred utility), the PMAC backup to an appropriate remote server. The PMAC backup files are saved in the following directory: /var/TKLC/smac/backup.</p> |

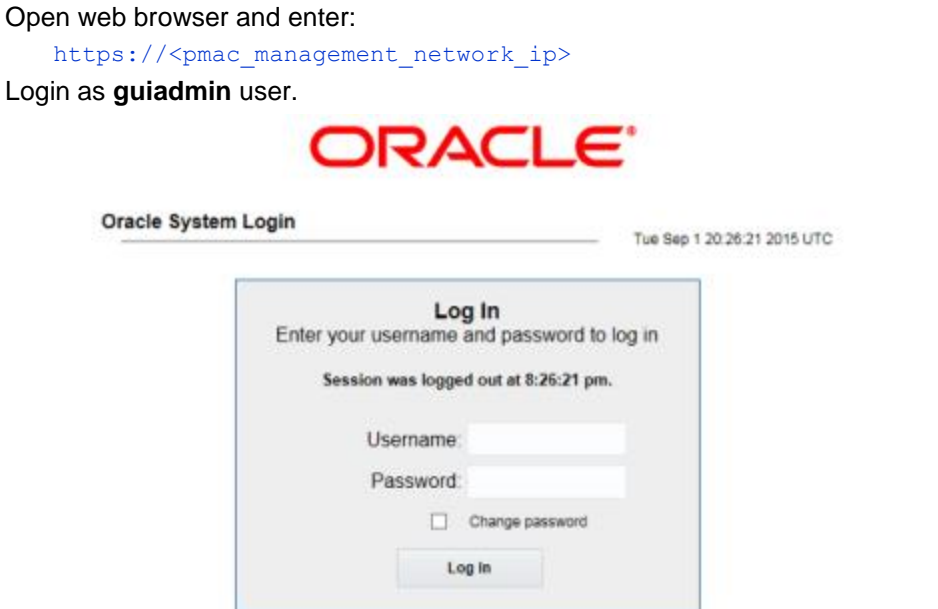
9.6 Add Cabinet and Enclosure to the PMAC System Inventory

This procedure adds a cabinet and an enclosure to the PMAC inventory.

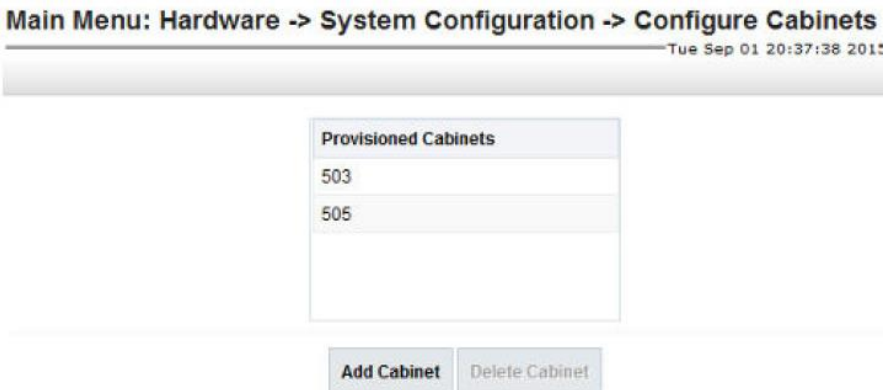
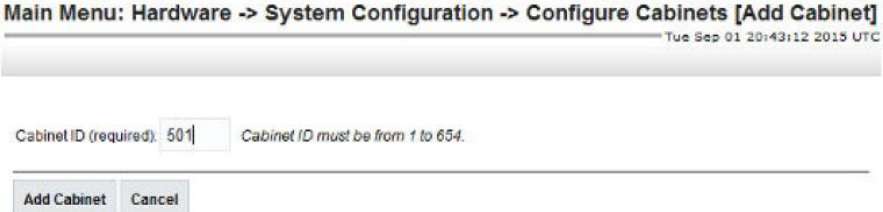
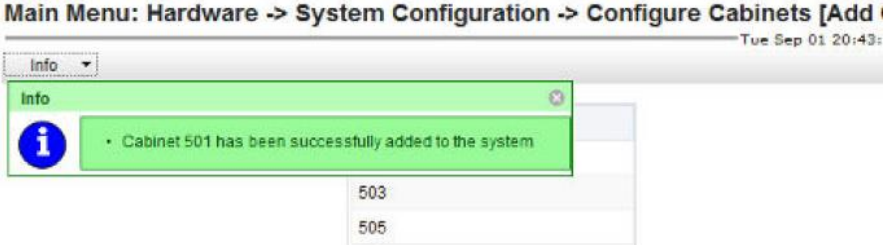
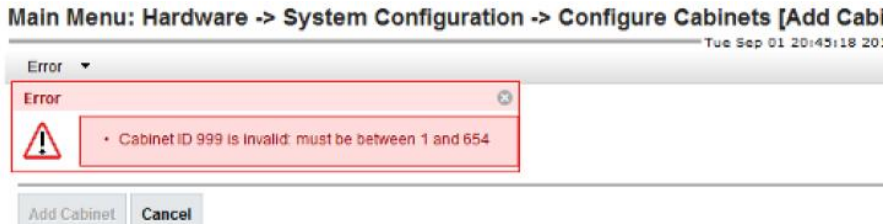
Prerequisite: 9.5 Configure PMAC Application

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.


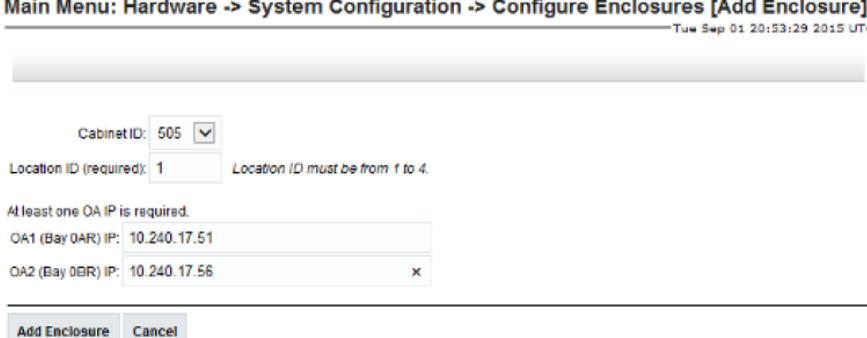
Procedure 59. Add Cabinet and Enclosure to the PMAC System Inventory

| Step | Procedure | Results |
|--------------------------------|---------------------------|---|
| 1. <input type="checkbox"/> | PMAC GUI: Login | Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.  |

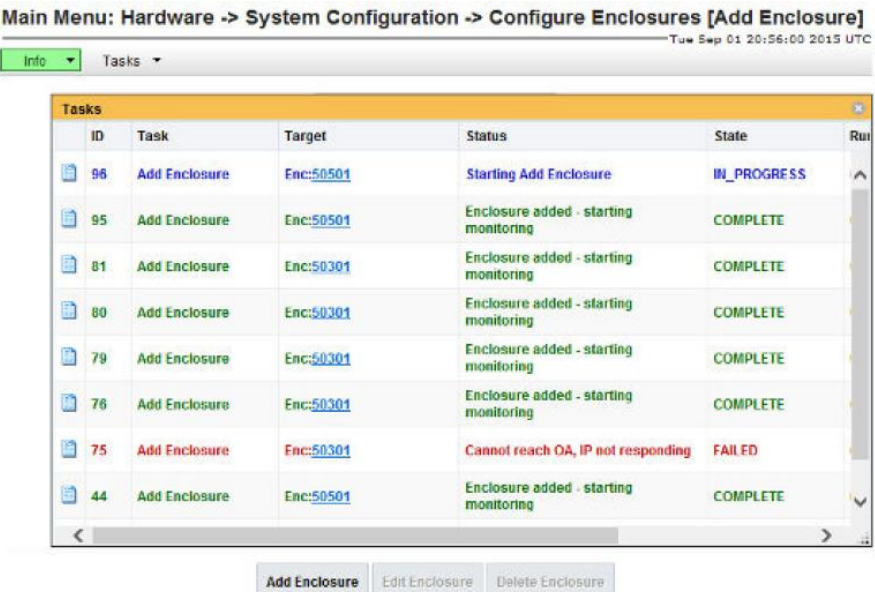
Procedure 59. Add Cabinet and Enclosure to the PMAC System Inventory

| Step | Procedure | Results |
|------------------------------------|--|--|
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Add cabinet</p> | <p>1. Navigate to Hardware > System Configuration > Configure Cabinets.</p> <p>2. Click Add Cabinet.</p>  <p>3. Type the Cabinet ID and click Add Cabinet.</p>  <p>4. Check for errors.</p> <p>Success:</p>  <p>Error:</p>  |
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Configure enclosures</p> | <p>1. Navigate to Hardware > System Configuration > Configure Enclosures.</p> <p>2. Click Add Enclosure.</p> |

Procedure 59. Add Cabinet and Enclosure to the PMAC System Inventory

| Step | Procedure | Results |
|------|-----------|---|
| | | <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures <small>Tue Sep 01 20:52:04 2015 UTC</small></p>  <p>3. Type the Cabinet ID, Location ID, and two OA IP addresses (the enclosure's active and standby OAs).</p> <p>4. Click Add Enclosure.</p> <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures [Add Enclosure] <small>Tue Sep 01 20:53:29 2015 UTC</small></p>  <p>Note Location ID is used to identify an enclosure within a cabinet. It can have a value of 1, 2, 3, or 4. The cabinet ID and location ID are combined to create a globally unique ID for the enclosure (for example, an enclosure in cabinet 502 at location 1, has an enclosure ID of 50201).</p> <p>5. The screen refreshes with a new background task entry. Click Tasks located on the toolbar under the Configure Enclosures heading.</p> |

Procedure 59. Add Cabinet and Enclosure to the PMAC System Inventory

| Step | Procedure | Results |
|------|-----------|---|
| | | <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures [Add Enclosure]</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |

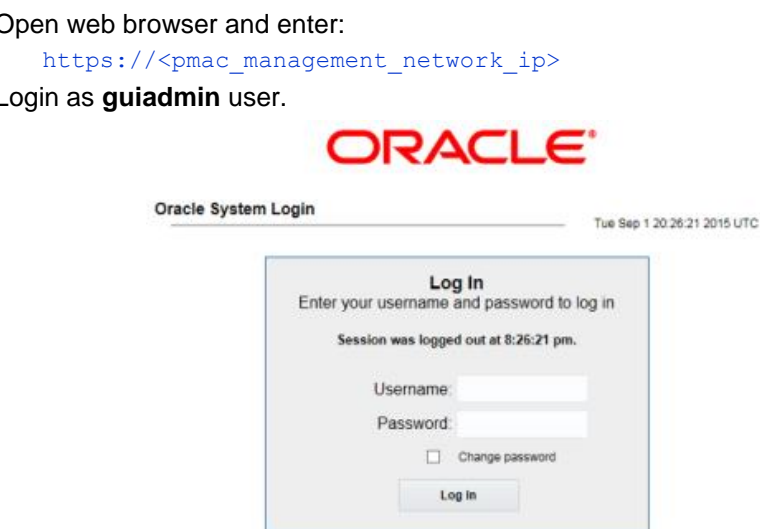
9.7 Edit an Enclosure in the PMAC System Inventory

This procedure edits an existing enclosure configuration in the PMAC system inventory. This is used to notify PMAC of enclosure OA IP address changes.

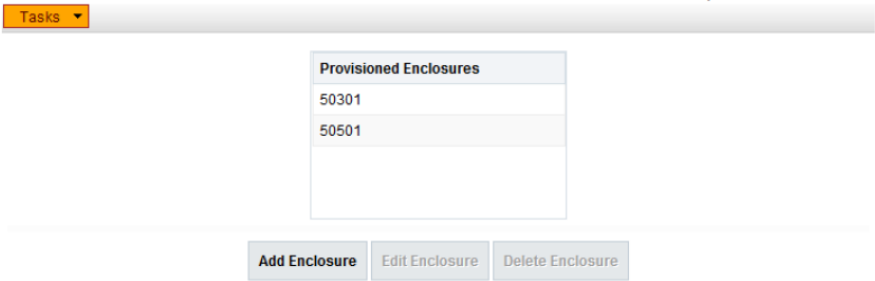
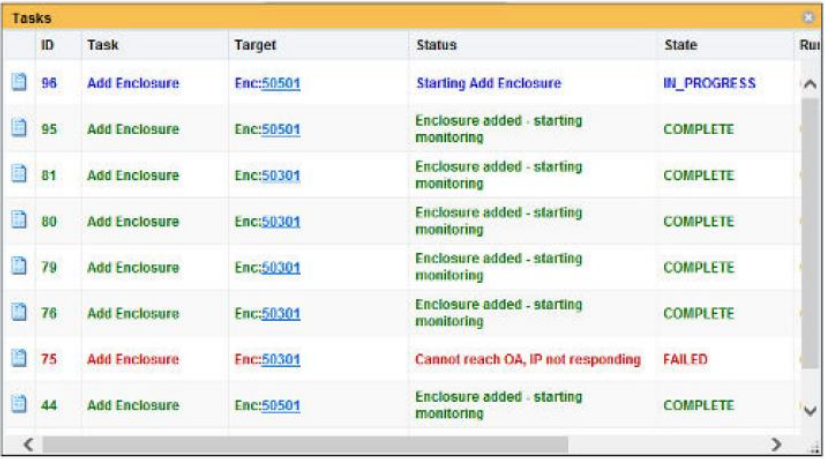
Prerequisite: 9.6 Add Cabinet and Enclosure to the PMAC System Inventory

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 60. Edit an Enclosure in the PMAC System Inventory

| Step | Procedure | Results |
|--------------------------------|---------------------------|--|
| 1. <input type="checkbox"/> | PMAC GUI: Login | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  |

Procedure 60. Edit an Enclosure in the PMAC System Inventory

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------------------------|---|---|---------------------------------------|-------------|--------|--------|-------|----|---------------|-----------|------------------------|-------------|----|---------------|-----------|---------------------------------------|----------|----|---------------|-----------|---------------------------------------|----------|----|---------------|-----------|---------------------------------------|----------|----|---------------|-----------|---------------------------------------|----------|----|---------------|-----------|---------------------------------------|----------|----|---------------|-----------|------------------------------------|--------|----|---------------|-----------|---------------------------------------|----------|
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Edit enclosures</p> | <ol style="list-style-type: none"> Navigate to Hardware > System Configuration > Configure Enclosures. Select a row from the list of provisioned enclosures and click Edit Enclosure. <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures Tue Sep 01 20:46:34 2015 UTC</p>  <ol style="list-style-type: none"> Modify the OA IP addresses as needed and click Edit Enclosure. <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures [Edit Enclosure 50501] Tue Sep 01 20:16:37 2015 UTC</p> <p>At least one OA IP is required. OA1 (Bay 0AR) IP: <input type="text" value="10.240.17.51"/> OA2 (Bay 0BR) IP: <input type="text" value="10.240.17.56"/></p> <p><input type="button" value="Edit Enclosure"/> <input type="button" value="Cancel"/></p> <ol style="list-style-type: none"> The screen refreshes with a new background task entry. Click Tasks located on the toolbar under the Configure Enclosures heading. <p>Main Menu: Hardware -> System Configuration -> Configure Enclosures [Add Enclosure] Tue Sep 01 20:56:00 2015 UTC</p>  <table border="1" data-bbox="560 1255 1380 1711"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>96</td> <td>Add Enclosure</td> <td>Enc:50501</td> <td>Starting Add Enclosure</td> <td>IN_PROGRESS</td> </tr> <tr> <td>95</td> <td>Add Enclosure</td> <td>Enc:50501</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> <tr> <td>81</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> <tr> <td>80</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> <tr> <td>79</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> <tr> <td>76</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> <tr> <td>75</td> <td>Add Enclosure</td> <td>Enc:50301</td> <td>Cannot reach OA, IP not responding</td> <td>FAILED</td> </tr> <tr> <td>44</td> <td>Add Enclosure</td> <td>Enc:50501</td> <td>Enclosure added - starting monitoring</td> <td>COMPLETE</td> </tr> </tbody> </table> <p><input type="button" value="Add Enclosure"/> <input type="button" value="Edit Enclosure"/> <input type="button" value="Delete Enclosure"/></p> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> | ID | Task | Target | Status | State | 96 | Add Enclosure | Enc:50501 | Starting Add Enclosure | IN_PROGRESS | 95 | Add Enclosure | Enc:50501 | Enclosure added - starting monitoring | COMPLETE | 81 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 80 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 79 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 76 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | 75 | Add Enclosure | Enc:50301 | Cannot reach OA, IP not responding | FAILED | 44 | Add Enclosure | Enc:50501 | Enclosure added - starting monitoring | COMPLETE |
| ID | Task | Target | Status | State | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 96 | Add Enclosure | Enc:50501 | Starting Add Enclosure | IN_PROGRESS | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 95 | Add Enclosure | Enc:50501 | Enclosure added - starting monitoring | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 81 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 76 | Add Enclosure | Enc:50301 | Enclosure added - starting monitoring | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 75 | Add Enclosure | Enc:50301 | Cannot reach OA, IP not responding | FAILED | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 44 | Add Enclosure | Enc:50501 | Enclosure added - starting monitoring | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

9.8 Add ISO Images to the PMAC Image Repository


This procedure adds ISO images to the PMAC repository.

Prerequisite: 9.5 Configure PMAC Application

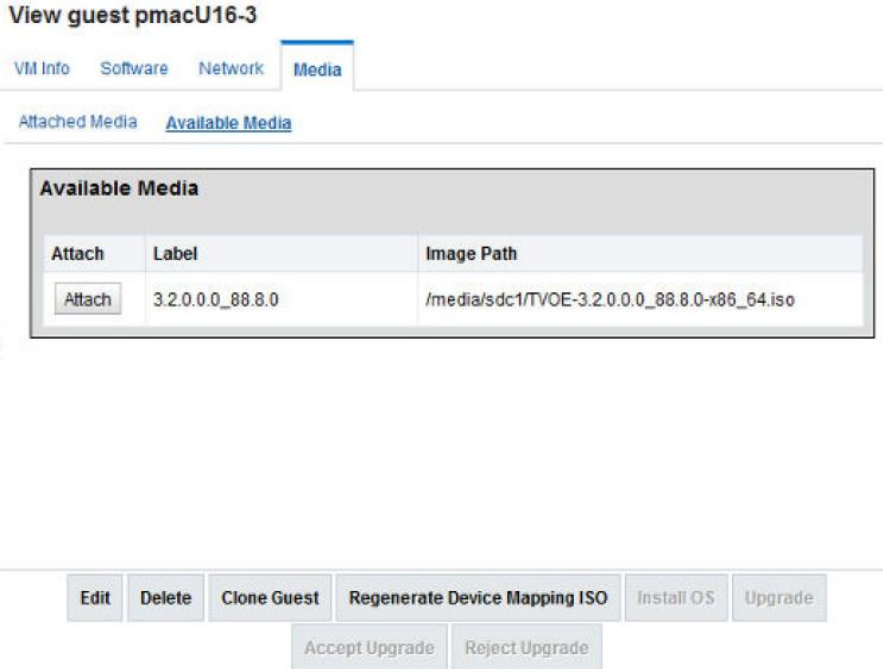
Note: If the ISO image has already been added to the PMAC software inventory in a previous procedure, skip this procedure.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

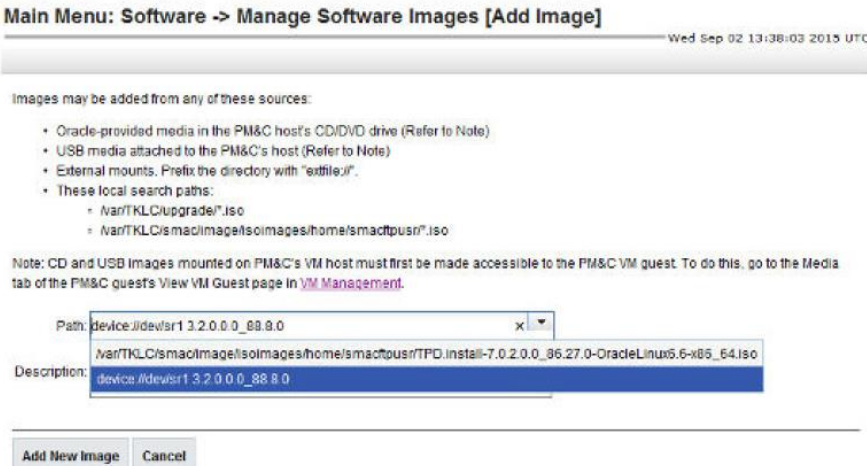
Procedure 61. Add ISO Images to the PMAC Image Repository

| Step | Procedure | Results |
|--|---|--|
| <p>1. <input type="checkbox"/></p> | <p>Make the image available to PMAC</p> | <p>There are two ways to make an image available to PMAC:</p> <ul style="list-style-type: none"> • Attach the USB device containing the ISO image to a USB port of the management server. • Use SFTP to transfer the iso image to the PMAC server in the /var/TKLC/smac/image/isoimages/home/smacftpusr/ directory as pmacftpusr user: <ul style="list-style-type: none"> • cd into the directory where your ISO image is located (not on the PMAC server) • Using SFTP, connect to the PMAC management server as the pmacftpusr user. If using IPv6, shell escapes around the IPv6 address may be required. <pre>> sftp pmacftpusr@<pmac_management_network_ip> > put <image>.iso</pre> • After the image transfer is 100% complete, close the connection <pre>> quit</pre> <p>Refer to the documentation provided by application for pmacftpusr password.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <code>https://<pmac_management_network_ip></code></p> <p>Login as guiadmin user.</p>  |

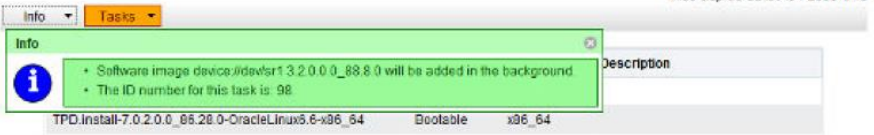
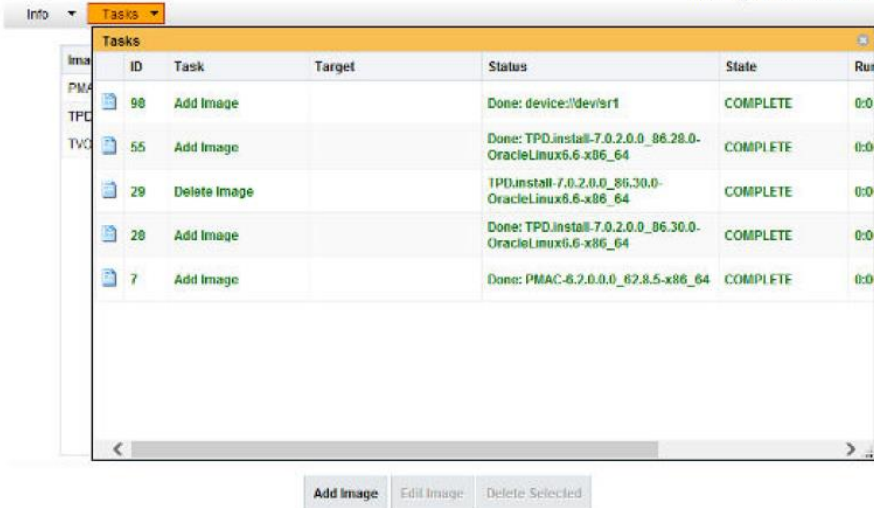
Procedure 61. Add ISO Images to the PMAC Image Repository

| Step | Procedure | Results | | | | | | | | | |
|---|---|---|-----------------|--|--|--------|-------|------------|---------------------------------------|------------------|--|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Attach software image to the PMAC guest</p> | <p>If in step 1 the ISO image was transferred directly to the PMAC guest using SFTP, skip this step and continue with the next step. If the image is on a USB device, continue with this step.</p> <ol style="list-style-type: none"> 1. Navigate to Main Menu > VM Management.. Select PMAC guest from the VM Entities list. 2. Click the Media tab. 3. Locate the ISO image in the Available Media list, and click Attach next to it. After a pause, the image displays in the Attached Media list.  <p>View guest pmacU16-3</p> <p>VM Info Software Network Media</p> <p>Attached Media <u>Available Media</u></p> <table border="1"> <thead> <tr> <th colspan="3">Available Media</th> </tr> <tr> <th>Attach</th> <th>Label</th> <th>Image Path</th> </tr> </thead> <tbody> <tr> <td><input type="button" value="Attach"/></td> <td>3.2.0.0.0_88.8.0</td> <td>/media/sdc1/TVOE-3.2.0.0.0_88.8.0-x86_64.iso</td> </tr> </tbody> </table> <p>Edit Delete Clone Guest Regenerate Device Mapping ISO Install OS Upgrade</p> <p>Accept Upgrade Reject Upgrade</p> | Available Media | | | Attach | Label | Image Path | <input type="button" value="Attach"/> | 3.2.0.0.0_88.8.0 | /media/sdc1/TVOE-3.2.0.0.0_88.8.0-x86_64.iso |
| Available Media | | | | | | | | | | | |
| Attach | Label | Image Path | | | | | | | | | |
| <input type="button" value="Attach"/> | 3.2.0.0.0_88.8.0 | /media/sdc1/TVOE-3.2.0.0.0_88.8.0-x86_64.iso | | | | | | | | | |

Procedure 61. Add ISO Images to the PMAC Image Repository

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Manage Software Image screen</p> | <ol style="list-style-type: none"> Navigate to Main Menu > Software > Manage Software Images. Click Add Image. <p>If in step 1 the ISO image was transferred directly to the PMAC guest using SFTP, it displays as a local file /var/TKLC/...</p> <p>If the image was supplied on a USB drive, it displays as a virtual device (device://...). These devices are assigned in numerical order as USB images become available on the management server. The first virtual device is reserved for internal use by TVOE and PMAC; therefore, the ISO image of interest is normally present on the second device, device://dev/sr1. If one or more USB-based images were already present on the management server before you started this procedure, select a correspondingly higher device number.</p> <ol style="list-style-type: none"> Type an image description and click Add New Image.  |

Procedure 61. Add ISO Images to the PMAC Image Repository

| Step | Procedure | Results |
|--|--|--|
| <p>5. <input type="checkbox"/></p> | <p>PMAC GUI: Monitor the status</p> | <p>Click Info to access the status and confirm a background task has been started to add the image.</p>  <p>Click Tasks located on the toolbar. Make sure the correct image or source device name displays in the Status column.</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |
| <p>6. <input type="checkbox"/></p> | <p>PMAC GUI: Detach image from PMAC guest</p> | <p>If the image was supplied on USB, return to the PMAC guest's Media tab, locate the image in the Attached Media list, and click Detach next to it.</p> <p>To confirm the new image has been detached, reload the page by reselecting the VM guest in the VM Entities list and navigate to Media > Attached Media subtab.</p> <p>This releases the virtual device for future use.</p> <p>Remove the USB device from the management server.</p> |
| <p>7. <input type="checkbox"/></p> | <p>Repeat</p> | <p>If there are additional ISO images to be provisioned on the PMAC, repeat the procedure with the appropriate ISO image data.</p> |

9.9 IPM Servers Using PMAC Application

This procedure installs TPD or TVOE using an image from the PMAC image repository.


Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for IPM have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for IPM have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- A bootable image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.
- The BIOS settings on the servers have been verified using 6.2 Confirm/Upgrade Blade Server BIOS Settings or Section 3.2 of [1] TPD Initial Product Manufacture Software Installation Procedure.

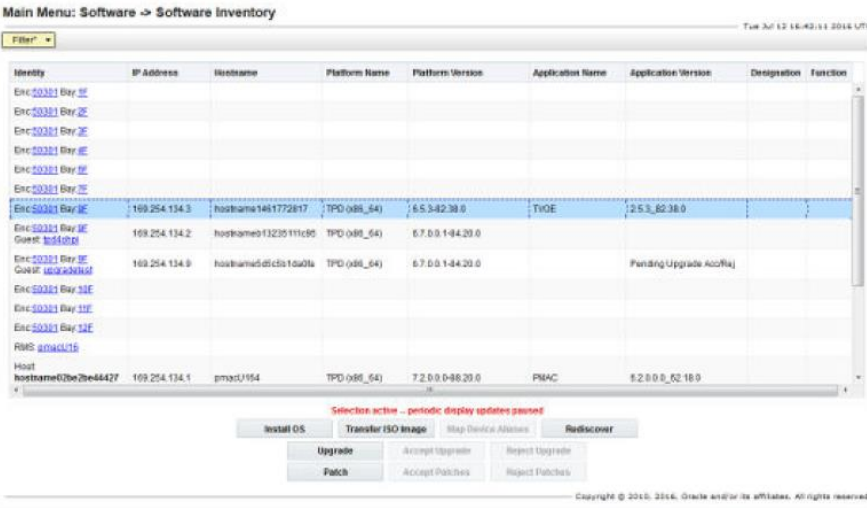
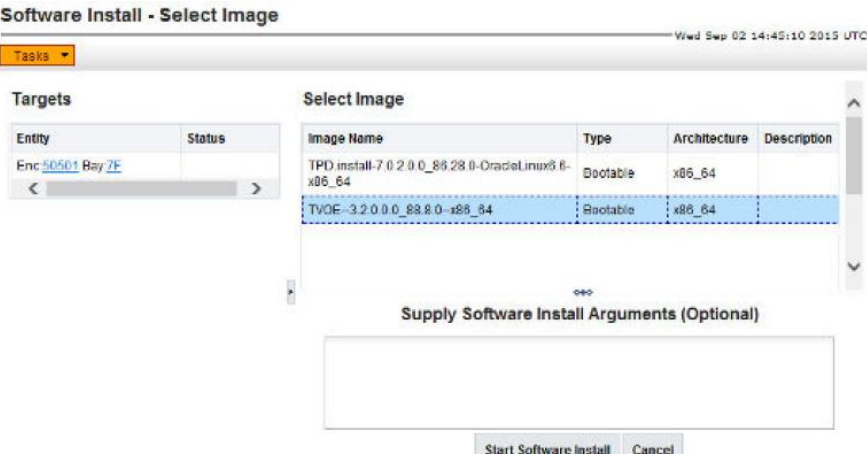
Note: If you are about to IPM as preparation for SAN configuration, follow 10.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.


Procedure 62. IPM Servers Using PMAC Application

| Step | Procedure | Results |
|--------------------------------|---------------------------|--|
| 1. <input type="checkbox"/> | PMAC GUI: Login | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  |

Procedure 62. IPM Servers Using PMAC Application

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|--|---------------|-------------------|------------------|------------------------|---|------------------|---------------------|-------------|------------------------------|-----------------|--------|--|--|--|--|--|--|--|-----------------|--|--|--|--|--|--|--|--|-----------------|--|--|--|--|--|--|--|--|-----------------|--|--|--|--|--|--|--|--|-----------------|--|--|--|--|--|--|--|--|-----------------|--|--|--|--|--|--|--|--|-----------------|---------------|--------------------|--------------|---------------|------|---------------|--|--|-----------------|---------------|---------------------|--------------|------------------|--|--|--|--|-----------------|---------------|----------------------|--------------|------------------|--|------------------------|--|--|-----------------|--|--|--|--|--|--|--|--|-----------------|--|--|--|--|--|--|--|--|-----------------|--|--|--|--|--|--|--|--|------|----------------------|----------|--------------|-------------------|------|-------------------|--|--|
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <ol style="list-style-type: none"> Navigate to Software > Software Inventory. Select the servers you want to IPM. If you want to install the same OS on more than one server, press Ctrl while selecting multiple rows. Click Install OS.  <p>Main Menu: Software -> Software Inventory</p> <table border="1"> <thead> <tr> <th>Identity</th> <th>IP Address</th> <th>Hostname</th> <th>Platform Name</th> <th>Platform Version</th> <th>Application Name</th> <th>Application Version</th> <th>Designation</th> <th>Function</th> </tr> </thead> <tbody> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td>169.254.134.3</td> <td>hostname1481772617</td> <td>TPD (x86_64)</td> <td>6.5.3-82.38.0</td> <td>TWOE</td> <td>2.5.3_82.38.0</td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td>169.254.134.2</td> <td>hostname61323011c96</td> <td>TPD (x86_64)</td> <td>6.7.0.0-184.20.0</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td>169.254.134.9</td> <td>hostnamead6f6c16a01a</td> <td>TPD (x86_64)</td> <td>6.7.0.0-184.20.0</td> <td></td> <td>Pending Upgrade Action</td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc50301 Bay 2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Host</td> <td>hostname67be7be44477</td> <td>pmac/154</td> <td>TPD (x86_64)</td> <td>7.2.0.0-0-88.20.0</td> <td>PMAC</td> <td>6.2.0.0_0_02.18.0</td> <td></td> <td></td> </tr> </tbody> </table> | Identity | IP Address | Hostname | Platform Name | Platform Version | Application Name | Application Version | Designation | Function | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | 169.254.134.3 | hostname1481772617 | TPD (x86_64) | 6.5.3-82.38.0 | TWOE | 2.5.3_82.38.0 | | | Enc50301 Bay 2E | 169.254.134.2 | hostname61323011c96 | TPD (x86_64) | 6.7.0.0-184.20.0 | | | | | Enc50301 Bay 2E | 169.254.134.9 | hostnamead6f6c16a01a | TPD (x86_64) | 6.7.0.0-184.20.0 | | Pending Upgrade Action | | | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | | | | | | | | | Enc50301 Bay 2E | | | | | | | | | Host | hostname67be7be44477 | pmac/154 | TPD (x86_64) | 7.2.0.0-0-88.20.0 | PMAC | 6.2.0.0_0_02.18.0 | | |
| Identity | IP Address | Hostname | Platform Name | Platform Version | Application Name | Application Version | Designation | Function | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | 169.254.134.3 | hostname1481772617 | TPD (x86_64) | 6.5.3-82.38.0 | TWOE | 2.5.3_82.38.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | 169.254.134.2 | hostname61323011c96 | TPD (x86_64) | 6.7.0.0-184.20.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | 169.254.134.9 | hostnamead6f6c16a01a | TPD (x86_64) | 6.7.0.0-184.20.0 | | Pending Upgrade Action | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc50301 Bay 2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Host | hostname67be7be44477 | pmac/154 | TPD (x86_64) | 7.2.0.0-0-88.20.0 | PMAC | 6.2.0.0_0_02.18.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Select image</p> | <ol style="list-style-type: none"> Select the OS image to install on the servers. (Optional) Install arguments can be supplied by entering them into the text box displayed under the list of bootable images. These arguments are appended to the kernel line during the IPM process. If no install arguments need to be supplied for the OS being installed, leave the install arguments text box empty. <p>Note: The valid arguments for a TPD IPM are listed in [1] TPD Initial Product Manufacture Software Installation Procedure.</p> <ol style="list-style-type: none"> Click Start Software Install.  <p>Software Install - Select Image</p> <table border="1"> <thead> <tr> <th>Image Name</th> <th>Type</th> <th>Architecture</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>TPD install-7.0.2.0.0_88.28.0-OracleLinux8.6-x86_64</td> <td>Bootable</td> <td>x86_64</td> <td></td> </tr> <tr> <td>TWOE-3.2.0.0_0_88.8.0-x86_64</td> <td>Bootable</td> <td>x86_64</td> <td></td> </tr> </tbody> </table> <p>Supply Software Install Arguments (Optional)</p> <p>Start Software Install Cancel</p> | Image Name | Type | Architecture | Description | TPD install-7.0.2.0.0_88.28.0-OracleLinux8.6-x86_64 | Bootable | x86_64 | | TWOE-3.2.0.0_0_88.8.0-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Image Name | Type | Architecture | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TPD install-7.0.2.0.0_88.28.0-OracleLinux8.6-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TWOE-3.2.0.0_0_88.8.0-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | | <ol style="list-style-type: none"> Click OK to confirm the install. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 62. IPM Servers Using PMAC Application

| Step | Procedure | Results |
|--------------------------------|--|---|
| 4. <input type="checkbox"/> | PMAC GUI: Monitor install OS | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Install OS background task. A separate task displays for each server.</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |
| 5. <input type="checkbox"/> | Repeat | Repeat this procedure for additional rack mount servers. |

9.10 Install/Upgrade Applications Using PMAC

This procedure installs upgrades an application using an image from the PMAC image repository.

Prerequisites:


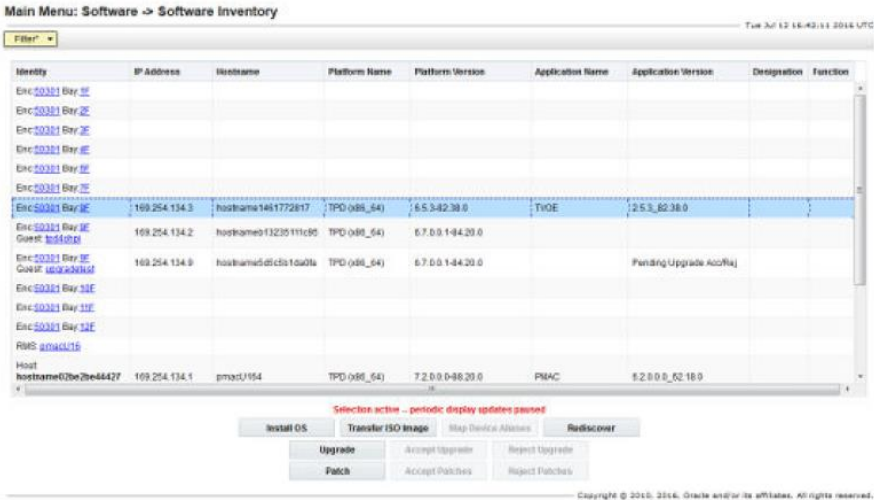
- Enclosures containing the blade servers or servers containing a TVOE host targeted for IPM have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for IPM have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- An upgradable image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.

Notes:

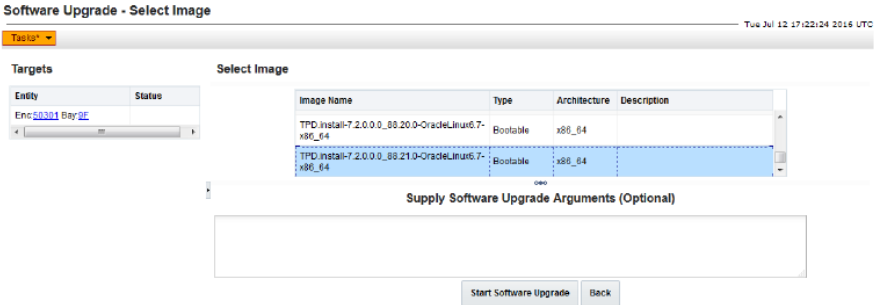
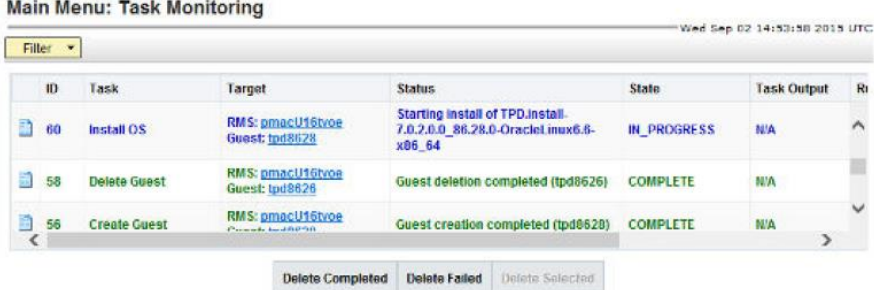
- Firmware update is only supported for HP c-Class blades and Rack Mount Servers.
- Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 63. Install/Upgrade Applications Using PMAC

| Step | Procedure | Results |
|------------------------------------|--|--|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <ol style="list-style-type: none"> Navigate to Software > Software Inventory. Select the servers you want to upgrade. If you want to upgrade more than one server, press Ctrl while selecting multiple rows. Click Upgrade.  <p>Note: Until the target servers are fully discovered by PMAC, you are unable to start an application install or upgrade on the servers (this may take up to 15 minutes after the OS Installs complete). A server that has not yet been discovered is represented by an empty row on the Software Inventory screen (no IP address, hostname, plat name, plat version, etc., displays).</p> |

Procedure 63. Install/Upgrade Applications Using PMAC

| Step | Procedure | Results |
|---|---|---|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Select image</p> | <p>1. Select the OS image to install on the servers.</p> <p>2. (Optional) Install arguments can be supplied by entering them into the text box displayed under the list of bootable images. These arguments are appended to the kernel line during the IPM process. If no install arguments need to be supplied for the OS being installed, leave the install arguments text box empty.</p> <p>Note: PMAC does not validate firmware update arguments.</p> <p>3. Click Start Software Upgrade.</p>  <p>4. Click OK to confirm the upgrade.</p> |
| <p>4.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Monitor upgrade</p> | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Upgrade background task. A separate task displays for each server.</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |
| <p>5.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI</p> | <p>Verify the installed/upgraded application is fully functional. The application must provide the steps for verifying its functionality.</p> |
| <p>6.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Accept or reject upgrade (platform 6.x applications only)</p> | <p>If the application you just upgraded or installed is based on a TPD release supported by PMAC 6.6, you must either accept or reject the upgrade. To accept an upgrade using PMAC, perform 9.18 Accept Upgrades Using PMAC . Likewise, to reject an upgrade using PMAC, perform 9.19 Reject Upgrades Using PMAC.</p> |

9.11 Patch Applications Using PMAC

This procedure patches an application using an image from the PMAC image repository.


Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host for an application patch have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for an application patch have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- A patch image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.
- Target servers have been IPM'd with an application based on a TPD 7.2 release.

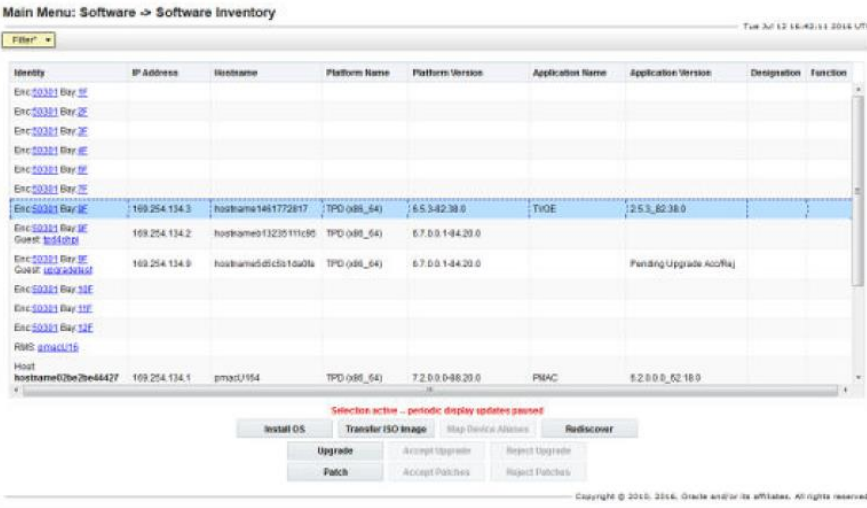
Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

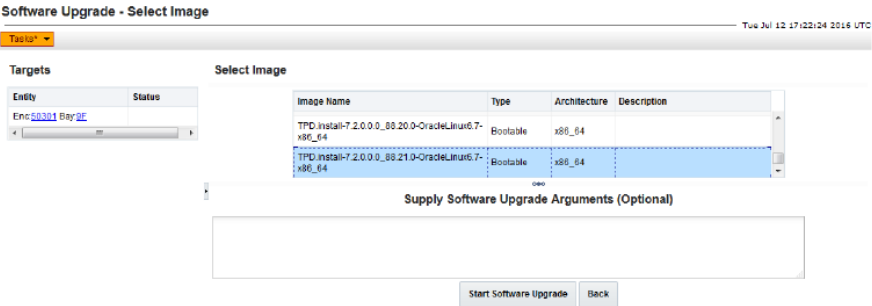
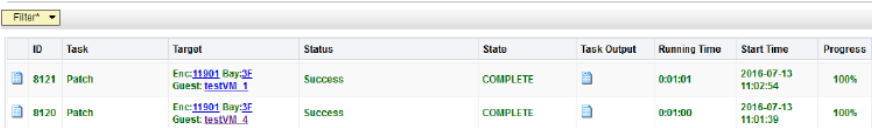
Procedure 64. Patch Applications Using PMAC

| Step | Procedure | Results |
|--------------------------------|---------------------------|--|
| 1. <input type="checkbox"/> | PMAC GUI: Login | Open web browser and enter: <code>https://<pmac_management_network_ip></code> Login as guiadmin user.  |

Procedure 64. Patch Applications Using PMAC

| Step | Procedure | Results |
|---|--|--|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <ol style="list-style-type: none"> Navigate to Software > Software Inventory. Select the servers you want to upgrade. If you want to upgrade more than one server, press Ctrl while selecting multiple rows. Click Patch.  <p>Note: Until the target servers are fully discovered by PMAC, you are unable to start an application install or upgrade on the servers (this may take up to 15 minutes after the OS Installs complete). A server that has not yet been discovered is represented by an empty row on the Software Inventory screen (no IP address, hostname, plat name, plat version, etc., displays).</p> |

Procedure 64. Patch Applications Using PMAC

| Step | Procedure | Results |
|--|---|---|
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Select image</p> | <p>1. Select the OS image to install on the servers.</p> <p>2. (Optional) There are three optional arguments that can be specified as part of a patch.</p> <p>The first option is Reboot. If this is enabled, the patched server reboots once the patch installation has completed. The second option is No runlevel change required. If this is enabled, the patched server does not transition from runlevel 4 to 3 before installing the patch. This means applications running on the server are not halted during the patch installation. The third option is Modify runlevel timeout. If this is enabled, a custom runlevel timeout can be specified in the box below this option. This timeout (in minutes) determines how long the patching process waits for a runlevel transition from 4 to 3 before the installation is aborted.</p> <p>Any of these options can be specified as the sole option. Additionally, Reboot and Modify runlevel timeout may be specified together. No runlevel change required cannot be specified with either of the other options.</p> <p>Note: PMAC does not validate firmware update arguments.</p> <p>3. Click Start Patch Installation.</p>  <p>4. Click OK to confirm proceeding with the patch.</p> |
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Monitor patch</p> | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Patch background task. A separate task displays for each server.</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |
| <p>5. <input type="checkbox"/></p> | <p>PMAC GUI</p> | <p>Verify the patch installation. The application must provide the steps for verifying its functionality.</p> |

Procedure 64. Patch Applications Using PMAC

| Step | Procedure | Results |
|--------------------------------|--|---|
| 6. <input type="checkbox"/> | PMAC GUI: Accept or reject patch | If the application you just patched is based on a TPD 7.2 release or later, you must accept or reject the upgrade. To accept a patch using PMAC, perform 9.20 Accept Patches Using PMAC. Likewise, to reject an upgrade using PMAC, perform 9.21 Reject Patches Using PMAC. |

9.12 Install PMAC on Redundant DL360 or DL380

This procedure installs and configures TVOE on a redundant DL360 or DL380 server, deploys a redundant PMAC, and creates the first backup from the primary PMAC.

This procedure is optional and required only if the redundant PMAC server feature is to be deployed.

Prerequisites:

- 9.8 Add ISO Images to the PMAC Image Repository has been completed using the TVOE media.
- 9.8 Add ISO Images to the PMAC Image Repository has been completed using the PMAC media. Note the PMAC image name; it is used during the procedure as <PMAC_Image_Name>.
- 9.9 IPM Servers Using PMAC Application has been completed on the redundant management server using the TVOE media.
- 9.2 Configure TVOE Network has been completed on the redundant management server.

Notes:

- In the event a disaster recovery is required, refer to the recovery procedure in 909-2210-001.
- It is assumed that the use of a redundant PMAC means the NetBackup feature is not in use.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.


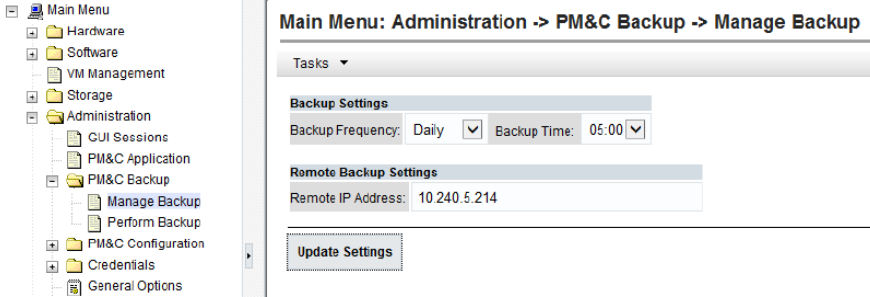
Procedure 65. Install PMAC on Redundant DL360 or DL380

| Step | Procedure | Results |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Redundant Management Server iLO: Login | <ol style="list-style-type: none"> 1. Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. <a href="http://<redundant_management_server_iLO_IP>">http://<redundant_management_server_iLO_IP> 2. Click on the Remote Console tab and open the Integrated Remote Console on the server. 3. Click Yes if the Security Alert displays. |

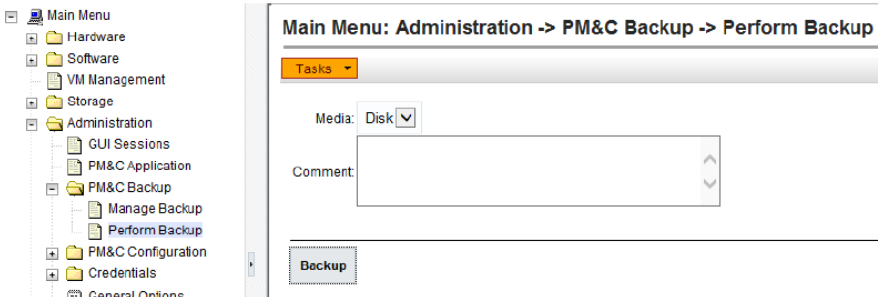
Procedure 65. Install PMAC on Redundant DL360 or DL380

| Step | Procedure | Results |
|--|---|--|
| <p>2. <input type="checkbox"/></p> | <p>Primary Management Server iLO: Log into the primary management server on the remote console</p> | <p>Log into PMAC with admusr credentials.</p> <p>Note: On a TVOE host, if you open the virsh console, for example, <code>\$ sudo /usr/bin/virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or the output is not correct, then there is likely a stuck virsh console command already being run on the TVOE host. Exit out of the virsh console, run <code>ps -ef grep virsh</code>, and then kill the existing process <code>kill -9 <PID></code>. Then execute the <code>virsh console X</code> command. Your console session should now run as expected.</p> <p>Login using virsh and wait until you see the login prompt. If a login prompt does not appear after the guest is finished booting, press Enter to make one appear:</p> <pre>\$ sudo /usr/bin/virsh virsh # list Id Name State 4 pmacU17-1 running virsh # console pmacU17-1 [Output Removed] pmacU17-1 login:</pre> |
| <p>3. <input type="checkbox"/></p> | <p>Primary PMAC: Export ISO image</p> | <p>Export the PMAC ISO image to the redundant management server's address on the control network.</p> <pre>\$ sudo /usr/sbin/exportfs <redundant_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name></pre> |
| <p>4. <input type="checkbox"/></p> | <p>Redundant Management Server TVOE: Mount media</p> | <p>Mount the PMAC upgrade media from the PMAC server.</p> <pre>\$ sudo /bin/mount <primary_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name> /mnt/upgrade</pre> |
| <p>5. <input type="checkbox"/></p> | <p>Redundant Management Server TVOE: Deploy PMAC instance</p> | <p>Using the pmac-deploy script, deploy the PMAC instance using the configuration detailed by the completed NAPD. All configuration options (NetBackup or isoimagesVolSizeGB) should match the configuration of the primary PMAC.</p> <p>For this example, a PMAC is deployed without NetBackup.</p> <pre>\$ cd /mnt/upgrade/upgrade \$ sudo ./pmac-deploy --guest=<Redundant_PMAC_Name> --hostname=<Redundant_PMAC_Name> -- controlBridge=<TVOE_Control_Bridge> --controlIP=<Redundant_PMAC_Control_ip_address> --controlNM=<PMAC_Control_netmask> --managementBridge=<PMAC_Management_Bridge> --managementIP=<Redundant_PMAC_Management_ip_address> --managementNM=<PMAC_Management_netmask_or_prefix> --routeGW=<PMAC_Management_gateway_address> --ntpserver=<Redundant_TVOE_Management_server_ip_address> --isoimagesVolSizeGB=20</pre> |

Procedure 65. Install PMAC on Redundant DL360 or DL380

| Step | Procedure | Results |
|---------------------------------|---|---|
| 6. <input type="checkbox"/> | <p>Redundant Management Server TVOE: Unmount the media and remove</p> | <p>After the PMAC deploys and boots, the management and control network comes up. At that point unmount the media and remove the PMAC media.</p> <pre>\$ cd / \$ sudo /bin/unmount /mmmnt/upgrade</pre> |
| 7. <input type="checkbox"/> | <p>Redundant PMAC</p> | <p>Perform 9.4 Set Up PMAC. WARNING: Initialization of the redundant PMAC is to be avoided at all costs.</p> |
| 8. <input type="checkbox"/> | <p>Primary PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  <p>Navigate to Administration > PMAC Backup > Manage Backup.</p> |
| 9. <input type="checkbox"/> | <p>Primary PMAC GUI: Configure primary PMAC to send backup to the redundant PMAC</p> | <p>Type the Remote IP Address of the redundant PMAC (redundant_management_server_mgmtVLAN_IP) and click Update Settings.</p>  |
| 10. <input type="checkbox"/> | <p>Primary PMAC GUI: Verify update was successful</p> | <p>Navigate to Task Monitoring. From the Background Task Monitoring view, verify the Update PMAC Backup Data task succeeds.</p> |

Procedure 65. Install PMAC on Redundant DL360 or DL380

| Step | Procedure | Results |
|---------------------------------|--|---|
| 11. <input type="checkbox"/> | Primary PMAC GUI: Perform initial backup to the redundant PMAC server | <p>Navigate to Administration > PMAC Backup > Perform Backup. Select Remote Server from the Media options, type any comments, and click Backup.</p>  |
| 12. <input type="checkbox"/> | Primary PMAC GUI: Verify update was successful | <p>Navigate to Task Monitoring. From the Background Task Monitoring view, verify the Backup PMAC task succeeds.</p> <p>This backup copies the existing PMAC backup files and all of the images added to the PMAC image repository from the primary PMAC server to the redundant PMAC server.</p> |
| 13. <input type="checkbox"/> | Primary PMAC: Unexport the PMAC ISO image | <pre>\$ sudo /usr/sbin/exportfs -u <redundant_pmac_control_ip>:/usr/TKLC/smac/html/TPD/<PMAC_Image_Name></pre> |

9.13 Configure Management Server SNMP Trap Target

This procedure configures SNMP settings for the management server.

Prerequisites:

- 9.5 Configure PMAC Application
- Know IP address of the target NMS for SNMP traps

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 66. Configure Management Server SNMP Trap Target

| Step | Results |
|--------------------------------|--|
| 1. <input type="checkbox"/> | Perform 12.3 Add SNMP Trap Destination on TPD-Based Application logging into the management server and providing the IP address of each trap destination. |
| 2. <input type="checkbox"/> | Ensure the PMAC specific MIB files are located in the /usr/TKLC/smac/etc/mib directory on the management server. The file of interest is pmacAppAlarms.mib. |

9.14 Install and Configure PMAC NetBackup Client

This procedure installs and configures the NetBackup client software on a PMAC application.

Prerequisite: The PMAC application must be initialized, or subsequent to the initialization configured with the NetBackup Feature enabled. Additionally the appropriate NetBackup network configuration for this system must be completed.

9.22 Initialize PMAC Application or 9.5 Configure PMAC Application

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 67. Install and Configure PMAC NetBackup Client

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | PMAC GUI | Verify the PMAC application guest has been configured with NetBackup virtual disk by following 9.22 Initialize PMAC Application. |
| 2. <input type="checkbox"/> | TVOE Management Server iLO: Login | <ol style="list-style-type: none"> Log into the management server iLO with Internet Explorer using the password provided by the application following Appendix E.1 Access a Server Console Remotely. <a href="http://<management_server_iLO_IP>">http://<management_server_iLO_IP> Click on the Remote Console tab and open the Integrated Remote Console on the server. Click Yes if the Security Alert displays. |
| 3. <input type="checkbox"/> | TVOE Application Server iLO: Login | <p>Log into PMAC with admusr credentials.</p> <p>Note: On a TVOE host, if you open the virsh console, for example, <code>\$ sudo /usr/bin/virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or the output is not correct, then there is likely a stuck virsh console command already being run on the TVOE host. Exit out of the virsh console, run <code>ps -ef grep virsh</code>, and then kill the existing process <code>kill -9 <PID></code>. Then execute the <code>virsh console X</code> command. Your console session should now run as expected.</p> <p>Login using virsh and wait until you see the login prompt. If a login prompt does not appear after the guest is finished booting, press Enter to make one appear:</p> <pre>\$ sudo /usr/bin/virsh virsh # list Id Name State 4 pmacU17-1 running virsh # console pmacU17-1 [Output Removed] pmacU17-1 login:</pre> |

Procedure 67. Install and Configure PMAC NetBackup Client

| Step | Procedure | Results |
|--|--------------------|--|
| <p>4. <input type="checkbox"/></p> | <p>PMAC</p> | <p>Perform 12.5 Install the NetBackup Client Application. The following data is required:</p> <ul style="list-style-type: none"> • Netbackup support: <ul style="list-style-type: none"> • PMAC 5.7.0 supports NetBackup client software versions 7.1 and 7.5. • PMAC 5.7.1 through PMAC 6.6 supports NetBackup client software versions 7.1, 7.5, and 7.6.x. • The PMAC is a 64-bit application. • The PMAC application NetBackup user is NetBackup. See appropriate documentation for the password. • The paths to the PMAC application software NetBackup notify scripts are: <ul style="list-style-type: none"> • /usr/TKLC/smac/sbin/bpstart_notify • /usr/TKLC/smac/sbin/bpend_notify • For the PMAC application the following is the NetBackup server policy files list: <ul style="list-style-type: none"> • /var/TKLC/smac/image/repository/*.iso • /var/TKLC/smac/backup/backupPmac*.pef <p>At the NetBackup server, the NetBackup policy(ies) can now be created to perform the NetBackup backups of the PMAC application.</p> |

9.15 Add Rack Mount Server to the PMAC System Inventory


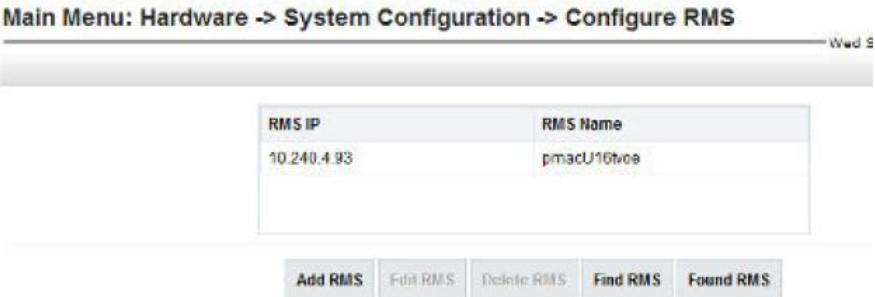
This procedure adds a rack mount server to the PMAC system inventory.

Prerequisite: 9.5 Configure PMAC Application

Note: You cannot edit the RMS iLO IP address. To change this address, delete and then add the RMS with the correct address.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

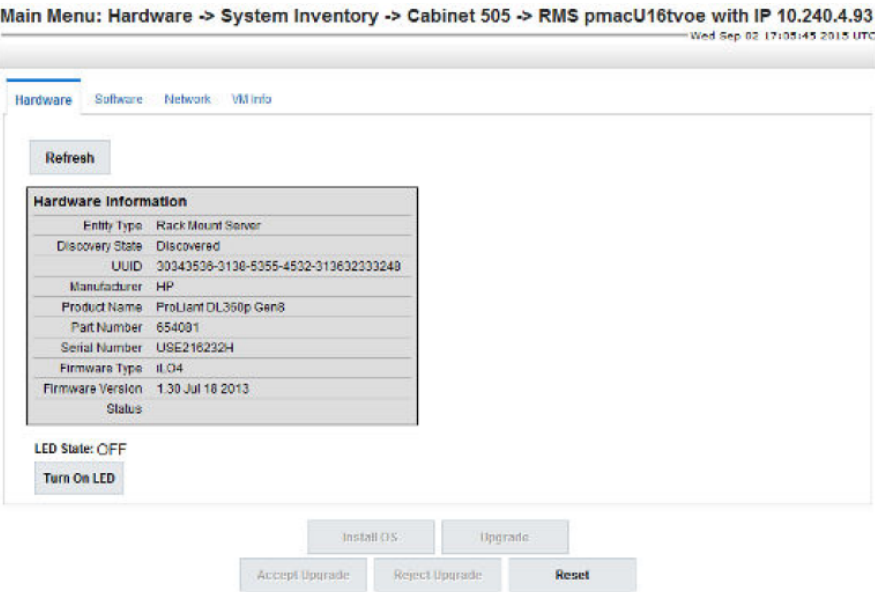
Procedure 68. Add Rack Mount Server to the PMAC System Inventory

| Step | Procedure | Results |
|--|--|--|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Add cabinet (optional)</p> | <p>If this is a RMS installation only or a cabinet has not been previously configured, perform step 2. of 9.6 Add Cabinet and Enclosure to the PMAC System Inventory to add one or more cabinets.</p> |
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Add RMS</p> | <p>1. Navigate to Hardware > System Configuration > Configure RMS. 2. Click Add RMS.</p>  <p>3. Type the IP address of the rack mount server management port (iLO) in the specified field. Type root as the User, type the Password for the iLO root user. All the other fields are optional. 4. Click Add RMS.</p> |

Procedure 68. Add Rack Mount Server to the PMAC System Inventory

| Step | Procedure | Results | | | | |
|-------------|-------------|---|--|----------|-------------|-------------|
| | | <p>Main Menu: Hardware -> System Configuration -> Configure RMS [Add RMS] Wed</p> <hr/> <p>IP (required): <input type="text" value="10.240.32.1"/> Name: <input type="text" value="appserver1"/> Cabinet ID: <input type="text" value="501"/> <input type="button" value="v"/> User: <input type="text"/> Password: <input type="password"/></p> <hr/> <p><input type="button" value="Add RMS"/> <input type="button" value="Cancel"/></p> <p>Note: If the initial iLO credentials provided by Oracle have been changed, enter valid credentials (not to be confused with OS or Application credentials) for the rack mount server management port.</p> <p>5. Check for errors.</p> <p>Success:</p> <p>Main Menu: Hardware -> System Configuration -> Configure RMS [Add RMS] Wed Sep 02 17</p> <p>Info <input type="button" value="v"/></p> <div style="border: 1px solid green; padding: 5px; margin-bottom: 10px;"> <p>Info <input type="button" value="x"/></p> <p> RMS 10.240.32.1 was added to the system.</p> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 50%;"></th> <th style="width: 50%;">RMS Name</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">10.240.4.93</td> <td>pmacU16tvoe</td> </tr> </tbody> </table> <p>Error:</p> <p>Main Menu: Hardware -> System Configuration -> Configure RMS [Add RMS] Wed Sep 02 17</p> <p>Error <input type="button" value="v"/></p> <div style="border: 1px solid red; padding: 5px; margin-bottom: 10px;"> <p>Error <input type="button" value="x"/></p> <p> Both the user and the password must be specified or neither.</p> </div> <p>Name: <input type="text"/></p> | | RMS Name | 10.240.4.93 | pmacU16tvoe |
| | RMS Name | | | | | |
| 10.240.4.93 | pmacU16tvoe | | | | | |

Procedure 68. Add Rack Mount Server to the PMAC System Inventory

| Step | Procedure | Results |
|------------------------------------|---|---|
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Verify RMS discovered</p> | <p>Navigate to Hardware > System Inventory > Cabinet xxx > RMS yyy where xxx is the cabinet ID selected when adding RMS (or unspecified) and yyy is the name of the RMS.</p> <p>Main Menu: Hardware -> System Inventory -> Cabinet 505 -> RMS pmacU16tvoe with IP 10.240.4.93 Wed Sep 02 17:05:45 2015 UTC</p>  <p>Click Refresh to refresh the hardware information periodically until the Discovery state changes from Undiscovered to Discovered. If Status displays an error, contact Error! Bookmark not defined. for assistance.</p> |


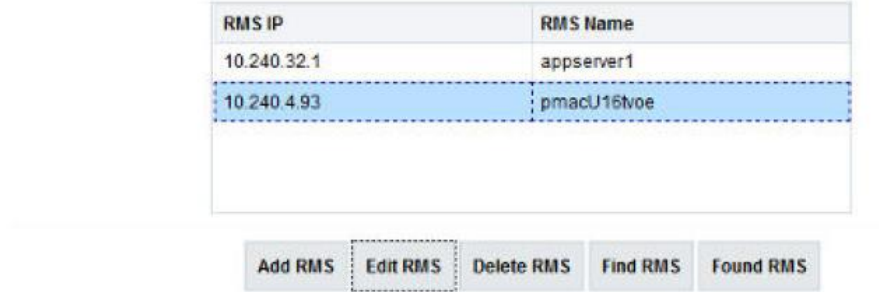
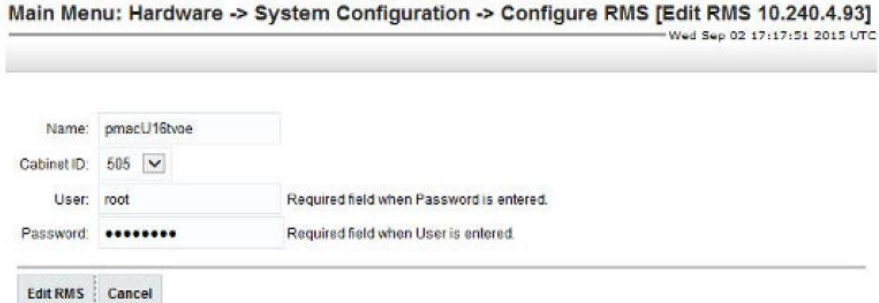
9.16 Edit Rack Mount Server in the PMAC System Inventory

This procedure edits a rack mount server in the PMAC system inventory. This procedure modifies the name, cabinet, or credentials of a provisioned RMS.

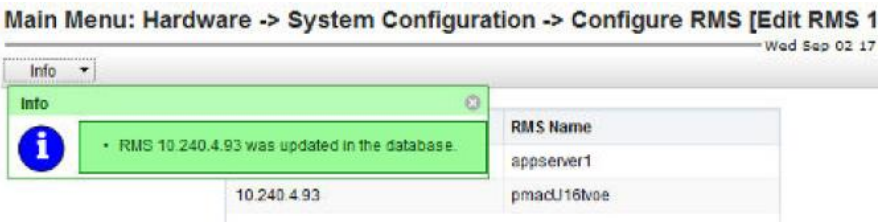
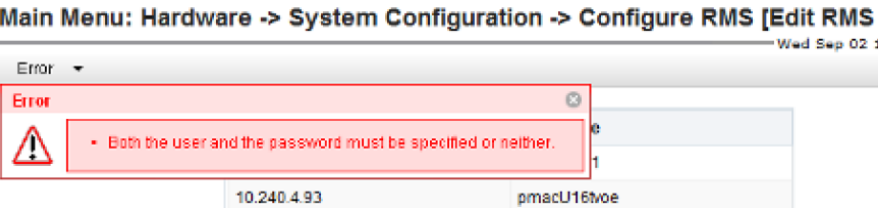
Prerequisite: 9.15 Add Rack Mount Server to the PMAC System Inventory

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 69. Edit Rack Mount Server in the PMAC System Inventory

| Step | Procedure | Results |
|--|--------------------------------------|---|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Edit RMS</p> | <ol style="list-style-type: none"> Navigate to Hardware > System Configuration > Configure RMS. Select one row in the list of rack mount servers and click Edit RMS.  <ol style="list-style-type: none"> Modify the fields that need to be changed. Click Edit RMS.  |

Procedure 69. Edit Rack Mount Server in the PMAC System Inventory

| Step | Procedure | Results |
|------|-----------|---|
| | | <p>5. Check for errors.</p> <p>Success:</p>  <p>Main Menu: Hardware -> System Configuration -> Configure RMS [Edit RMS 1] Wed Sep 02 17</p> <p>Info</p> <p>Info</p> <p>• RMS 10.240.4.93 was updated in the database.</p> <p>10.240.4.93</p> <p>RMS Name</p> <p>appserver1</p> <p>pmacU16tvoe</p> <p>Error:</p>  <p>Main Menu: Hardware -> System Configuration -> Configure RMS [Edit RMS] Wed Sep 02 17</p> <p>Error</p> <p>Error</p> <p>• Both the user and the password must be specified or neither.</p> <p>10.240.4.93</p> <p>pmacU16tvoe</p> |


9.17 Find and Add a Rack Mount Server to the PMAC System Inventory

This procedure locates and adds a RMS to the PMAC system inventory. Use this procedure to find rack mount servers running a Tekelec OS or within a specified IP address range and then add those to the PMAC system inventory.


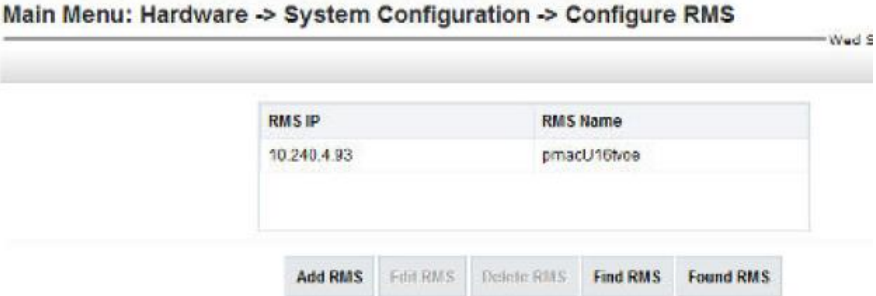
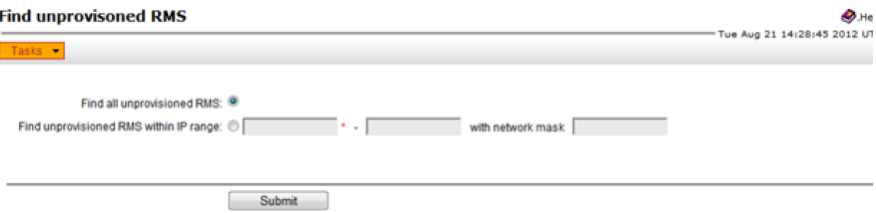
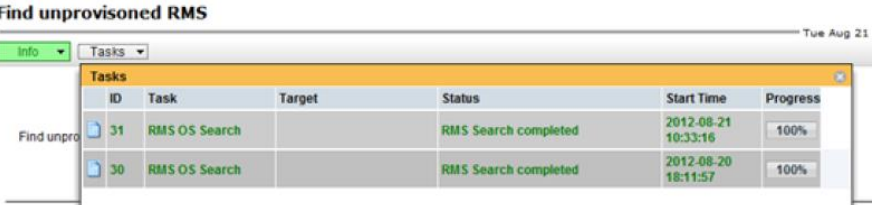
Prerequisite: 9.5 Configure PMAC Application

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.


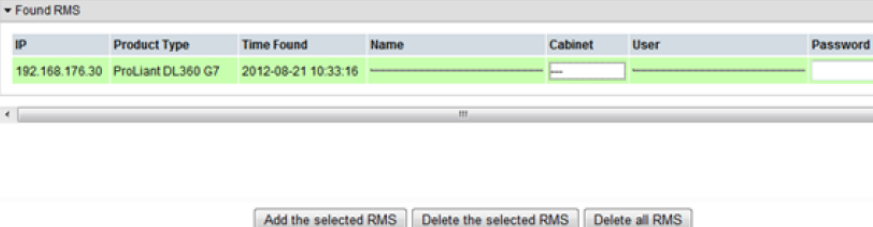
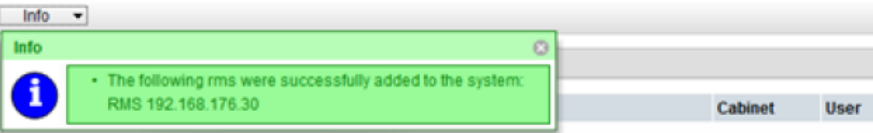
Procedure 70. Find and Add a Rack Mount Server to the PMAC System Inventory

| Step | Procedure | Results |
|-----------------|-----------------------------------|--|
| <p>1. □</p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  <p>Navigate to Administration > PMAC Configuration.</p> |

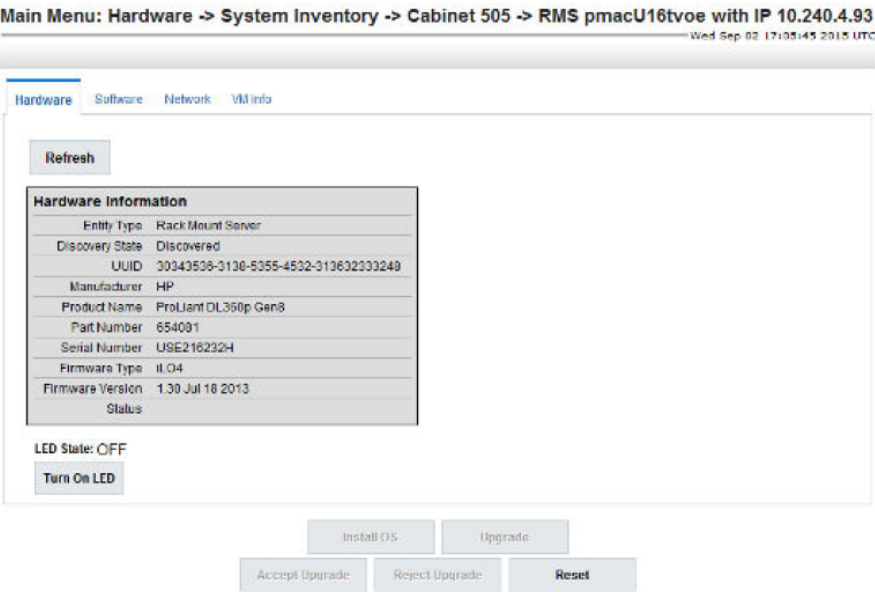
Procedure 70. Find and Add a Rack Mount Server to the PMAC System Inventory

| Step | Procedure | Results |
|---|--------------------------------------|---|
| <p>2. </p> | <p>PMAC GUI: Find RMS</p> | <ol style="list-style-type: none"> Navigate to Hardware > System Configuration > Configure RMS. Click Find RMS.  <ol style="list-style-type: none"> Select the type of find to perform. If the RMS has a Tekelec OS installed, then select the default Find all unprovisioned RMS. If the RMS does not have a Tekelec OS installed, then PMAC can search a range of IP addresses for a valid management port (for example, iLO) connection. Click Submit.  <ol style="list-style-type: none"> Monitor screen. The screen refreshes with a new background task entry. Click Tasks located on the toolbar under the Find unprovisioned RMS heading.  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |

Procedure 70. Find and Add a Rack Mount Server to the PMAC System Inventory

| Step | Procedure | Results |
|---|---|---|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Add found RMS</p> | <p>1. Click Found RMS.</p> <p>Main Menu: Hardware -> System Configuration -> Configure RMS</p>  <p>2. Select one of the servers and enter values for any optional fields, as needed</p> <p>3. Click Add the selected RMS.</p> <p>Found RMS</p>  <p>4. Check for errors.</p> <p>Found RMS</p>  |

Procedure 70. Find and Add a Rack Mount Server to the PMAC System Inventory

| Step | Procedure | Results |
|------------------------------------|---|---|
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Verify RMS discovered</p> | <p>Navigate to Hardware > System Inventory > Cabinet xxx > RMS yyy where xxx is the cabinet ID selected when adding RMS (or unspecified) and yyy is the name of the RMS.</p> <p>Main Menu: Hardware -> System Inventory -> Cabinet 505 -> RMS pmacU16tvoe with IP 10.240.4.93 Wed Sep 02 17:05:45 2015 UTC</p>  <p>Click Refresh to refresh the hardware information periodically until the Discovery state changes from Undiscovered to Discovered. If Status displays an error, contact Error! Bookmark not defined. for assistance.</p> |

9.18 Accept Upgrades Using PMAC

This procedure accepts upgrades using PMAC.


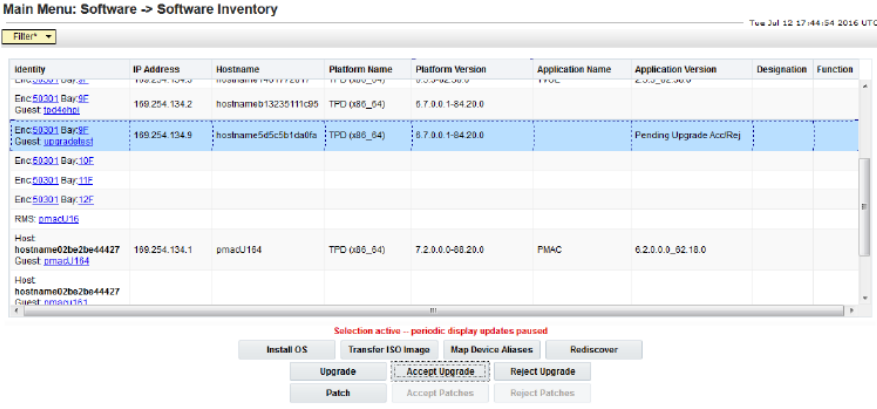
Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for accept upgrade have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for accept upgrade have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- The BIOS settings on the target servers have been verified using 6.2 Confirm/Upgrade Blade Server BIOS Settings or Section 3.2 of [1] TPD Initial Product Manufacture Software Installation Procedure.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 71. Accept Upgrades Using PMAC

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  <p>Navigate to Software > Software Inventory.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <p>To accept upgrades, the servers must be in the pending accept/reject upgrade state. Servers in this state have Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej state after an upgrade completes.</p> <ol style="list-style-type: none"> 1. Select the servers you want to upgrade. If you want to upgrade more than one server, press Ctrl while selecting multiple rows. 2. Click Accept Upgrade.  <p>Note: The servers may reboot if a migration of the file system is required.</p> <p>3. Click OK to confirm proceeding with the upgrade.</p> |

Procedure 71. Accept Upgrades Using PMAC

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|-------------------------------------|---|--|-------------|--------|--------|-------|------|---|----------------|----------------------------------|---------------------------------|-------------|------|---|------------|----------------------------------|----------|----------|----|---|------------|----------------------------------|--|----------|----|---|---------|----------------------------------|---------|----------|----|---|-------------|--|------------------------|----------|------|
| 3. <input type="checkbox"/> | PMAC GUI: Monitor upgrade | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Upgrade background task. A separate task displays for each server.</p> <p>Main Menu: Task Monitoring Wed Sep 02 20:25:58 2015 UTC</p> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Task</th> </tr> </thead> <tbody> <tr> <td>9</td> <td>Accept Upgrade</td> <td>Enc:50301 Bay:9F Guest: test3</td> <td>Task ID Assigned : 1438282870.0</td> <td>IN_PROGRESS</td> <td>N/ ^</td> </tr> <tr> <td>8</td> <td>Install OS</td> <td>Enc:50301 Bay:9F Guest: test4</td> <td>Canceled</td> <td>CANCELED</td> <td>N/</td> </tr> <tr> <td>7</td> <td>Install OS</td> <td>Enc:50301 Bay:9F Guest: test4</td> <td>Done: TPD.install-7.2.0.0_88.7.0-OracleLinux6.6-x86_64</td> <td>COMPLETE</td> <td>N/</td> </tr> <tr> <td>6</td> <td>Upgrade</td> <td>Enc:50301 Bay:9F Guest: test3</td> <td>Success</td> <td>COMPLETE</td> <td>N/</td> </tr> <tr> <td>5</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/ v</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Delete Completed"/> <input type="button" value="Delete Failed"/> <input type="button" value="Delete Selected"/> </p> </div> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> | ID | Task | Target | Status | State | Task | 9 | Accept Upgrade | Enc:50301 Bay:9F Guest: test3 | Task ID Assigned : 1438282870.0 | IN_PROGRESS | N/ ^ | 8 | Install OS | Enc:50301 Bay:9F Guest: test4 | Canceled | CANCELED | N/ | 7 | Install OS | Enc:50301 Bay:9F Guest: test4 | Done: TPD.install-7.2.0.0_88.7.0-OracleLinux6.6-x86_64 | COMPLETE | N/ | 6 | Upgrade | Enc:50301 Bay:9F Guest: test3 | Success | COMPLETE | N/ | 5 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/ v |
| ID | Task | Target | Status | State | Task | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | Accept Upgrade | Enc:50301 Bay:9F Guest: test3 | Task ID Assigned : 1438282870.0 | IN_PROGRESS | N/ ^ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | Install OS | Enc:50301 Bay:9F Guest: test4 | Canceled | CANCELED | N/ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | Install OS | Enc:50301 Bay:9F Guest: test4 | Done: TPD.install-7.2.0.0_88.7.0-OracleLinux6.6-x86_64 | COMPLETE | N/ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | Upgrade | Enc:50301 Bay:9F Guest: test3 | Success | COMPLETE | N/ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/ v | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

9.19 Reject Upgrades Using PMAC

This procedure rejects upgrades using PMAC.

Prerequisites:


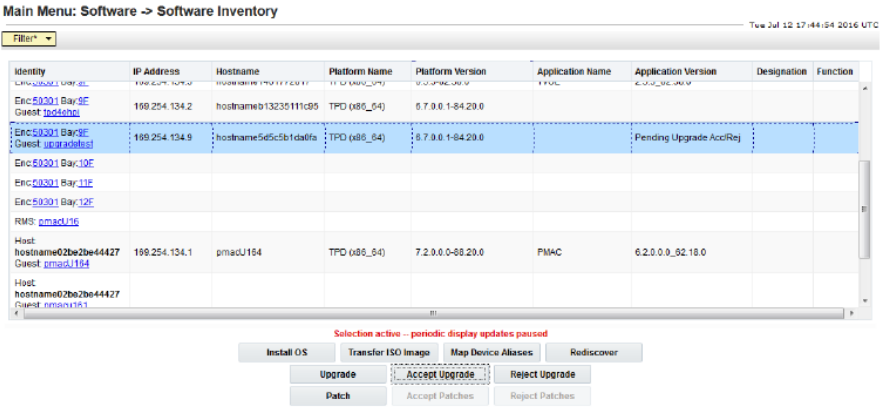
- Enclosures containing the blade servers or servers containing a TVOE host targeted for reject upgrade have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for reject upgrade have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

Notes:

- Until the target servers are fully discovered by PMAC, you are unable to reject upgrades on the servers (this may take up to 15 minutes after the upgrades complete).
- The image transfer is only supported for discovered entities (IP address is known)

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 72. Reject Upgrades Using PMAC

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  <p>Navigate to Software > Software Inventory.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <p>To reject upgrades, the servers must be in the pending accept/reject upgrade state. Servers in this state have Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej state after an upgrade completes.</p> <ol style="list-style-type: none"> 1. Select the servers with upgrades you want to reject. If you want to reject an upgrade on more than one server, press Ctrl while selecting multiple rows. 2. Click Reject Upgrade.  <p>3. Click OK to confirm proceeding with rejecting the upgrade.</p> |

Procedure 72. Reject Upgrades Using PMAC

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|-------------------------------------|---|---------------------------------|-------------|--------|--------|-------|------|---|----------------|----------------------------------|---------------------------------|-------------|------|---|---------|----------------------------------|---------|----------|------|----|---------|----------------------------------|---------|----------|------|----|---------|----------------------------------|---------|----------|------|----|---------|----------------------------------|---------|----------|------|
| 3. <input type="checkbox"/> | PMAC GUI: Monitor upgrade | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Reject Upgrade background task. A separate task displays for each server.</p> <p>Main Menu: Task Monitoring Wed Sep 02 20:29:12 2015 UTC</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Filter ▾</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Task</th> </tr> </thead> <tbody> <tr> <td>9</td> <td>Reject Upgrade</td> <td>Enc:50301 Bay:9E Guest: test3</td> <td>Task ID Assigned : 1438282870.0</td> <td>IN_PROGRESS</td> <td>N/ ^</td> </tr> <tr> <td>6</td> <td>Upgrade</td> <td>Enc:50301 Bay:9E Guest: test3</td> <td>Success</td> <td>COMPLETE</td> <td>100%</td> </tr> <tr> <td>15</td> <td>Upgrade</td> <td>Enc:50301 Bay:1E Guest: test2</td> <td>Success</td> <td>COMPLETE</td> <td>100%</td> </tr> <tr> <td>26</td> <td>Upgrade</td> <td>Enc:50301 Bay:9E Guest: test3</td> <td>Success</td> <td>COMPLETE</td> <td>100%</td> </tr> <tr> <td>29</td> <td>Upgrade</td> <td>Enc:50301 Bay:1E Guest: test2</td> <td>Success</td> <td>COMPLETE</td> <td>100%</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Delete Completed"/> <input type="button" value="Delete Failed"/> <input type="button" value="Delete Selected"/> </p> </div> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> | ID | Task | Target | Status | State | Task | 9 | Reject Upgrade | Enc:50301 Bay:9E Guest: test3 | Task ID Assigned : 1438282870.0 | IN_PROGRESS | N/ ^ | 6 | Upgrade | Enc:50301 Bay:9E Guest: test3 | Success | COMPLETE | 100% | 15 | Upgrade | Enc:50301 Bay:1E Guest: test2 | Success | COMPLETE | 100% | 26 | Upgrade | Enc:50301 Bay:9E Guest: test3 | Success | COMPLETE | 100% | 29 | Upgrade | Enc:50301 Bay:1E Guest: test2 | Success | COMPLETE | 100% |
| ID | Task | Target | Status | State | Task | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | Reject Upgrade | Enc:50301 Bay:9E Guest: test3 | Task ID Assigned : 1438282870.0 | IN_PROGRESS | N/ ^ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | Upgrade | Enc:50301 Bay:9E Guest: test3 | Success | COMPLETE | 100% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 15 | Upgrade | Enc:50301 Bay:1E Guest: test2 | Success | COMPLETE | 100% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 26 | Upgrade | Enc:50301 Bay:9E Guest: test3 | Success | COMPLETE | 100% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 29 | Upgrade | Enc:50301 Bay:1E Guest: test2 | Success | COMPLETE | 100% | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

9.20 Accept Patches Using PMAC

This procedure accepts patches using PMAC.


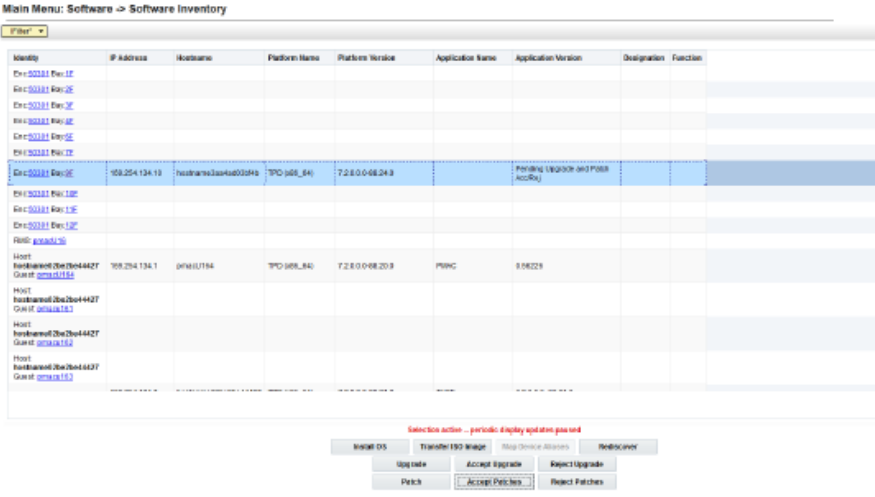
Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for the application patch have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for the application patch have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

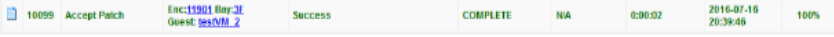
Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 73. Accept Patches Using PMAC

| Step | Procedure | Results |
|------------------------------------|--|---|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  <p>Navigate to Software > Software Inventory.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <p>To accept patches, the servers must be in the pending accept/reject state. Servers in this state have Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej state after an upgrade completes.</p> <ol style="list-style-type: none"> 1. Select the servers you want to patch. If you want to patch more than one server, press Ctrl while selecting multiple rows. 2. Click Accept Patches.  <ol style="list-style-type: none"> 3. Click OK to confirm proceeding with the patch. |

Procedure 73. Accept Patches Using PMAC

| Step | Procedure | Results |
|--------------------------------|--|--|
| 3. <input type="checkbox"/> | PMAC GUI: Monitor accept patch | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Patch background task. A separate task displays for each server.</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |

9.21 Reject Patches Using PMAC

This procedure rejects patches using PMAC.


Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for the application patch have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for the application patch have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- Target servers have been installed with an application based on a TPD release supported by PMAC 6.6.

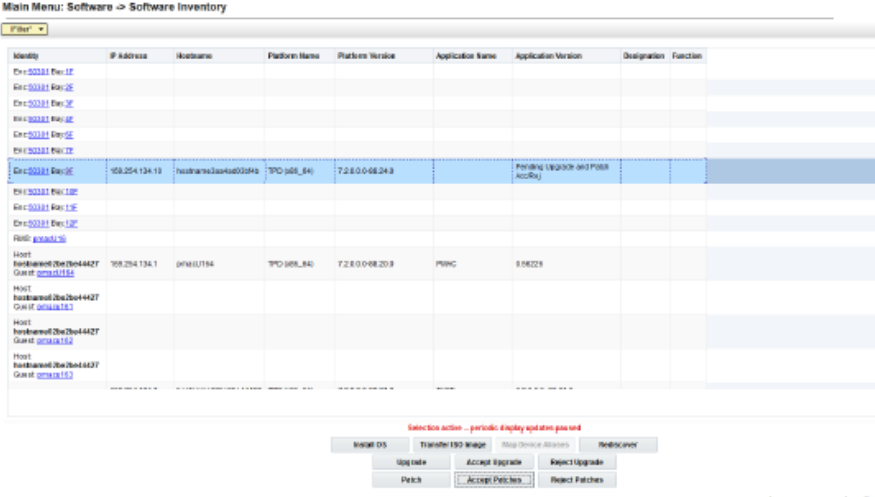
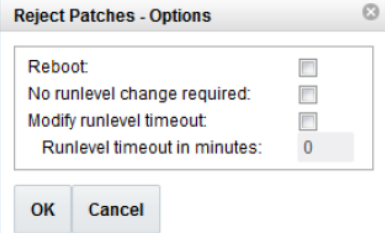
Note: Until the target servers are fully discovered by PMAC, you are unable to install patches on the servers (this may take up to 15 minutes after the upgrades complete).

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

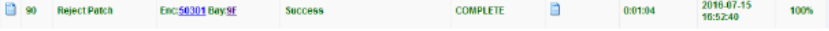
Procedure 74. Reject Patches Using PMAC

| Step | Procedure | Results |
|--------------------------------|---------------------------|--|
| 1. <input type="checkbox"/> | PMAC GUI: Login | <p>Open web browser and enter: <code>https://<pmac_management_network_ip></code> Login as guiadmin user.</p>  <p>Navigate to Software > Software Inventory.</p> |

Procedure 74. Reject Patches Using PMAC

| Step | Procedure | Results |
|---|--|--|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <p>To reject patches, the servers must be in the pending accept/reject state. Servers in this state have Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej displayed in their App Version column. It may take up to 15 minutes for PMAC to discover and display the Pending Upgrade Acc/Rej or Pending Upgrade and Patch Acc/Rej state after an upgrade completes.</p> <ol style="list-style-type: none"> 1. Select the servers with patches you want to reject. If you want to reject a patch on more than one server, press Ctrl while selecting multiple rows. 2. Click Reject Patches.  <p>3. (Optional) There are three optional arguments that can be specified as part of a patch rejection.</p> <p>The first option is Reboot. If this is enabled, the patched server reboots once the patch rejection has completed. The second option is No runlevel change required. If this is enabled, the patched server does not transition from runlevel 4 to 3 before rejecting the patch. This means applications running on the server are not halted during the patch rejection. The third option is Modify runlevel timeout. If this is enabled, a custom runlevel timeout can be specified in the box below this option. This timeout (in minutes) determines how long the patch rejection process waits for a runlevel transition from 4 to 3 before the rejection is aborted.</p> <p>Any of these options can be specified as the sole option. Additionally, Reboot and Modify runlevel timeout may be specified together. No runlevel change required cannot be specified with either of the other options.</p>  <ol style="list-style-type: none"> 4. Click OK to confirm proceeding with the rejecting the patch. |

Procedure 74. Reject Patches Using PMAC

| Step | Procedure | Results |
|--------------------------------|--|---|
| 3. <input type="checkbox"/> | PMAC GUI: Monitor reject patch | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Reject Patch background task. A separate task displays for each server.</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |

9.22 Initialize PMAC Application

This procedure initializes the PMAC application and network resources.

Initialization of the PMAC application can be performed using the PMAC CLI if an initialization profile exists with the desired features. In the case where a PMAC feature needs to be enabled or modified, the PMAC GUI is used to initialize the application.

Prerequisites:

- PMAC has been deployed and is not initialized or fully configured.
- Aggregation switches have been properly configured.

Notes:

- The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.
- If the NetBackup feature is to be configured on this PMAC, perform 9.22.2 Initialize PMAC Application Using the GUI.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

If the PMAC application is to be initialized using the PMAC CLI, perform 9.22.1 Initialize PMAC Application Using CLI; otherwise, perform 9.22.2 Initialize PMAC Application Using the GUI.

9.22.1 Initialize PMAC Application Using CLI

This procedure initializes the PMAC application and network resources using CLI.

Prerequisites:

- PMAC has been deployed and is not initialized or fully configured.
- Aggregation switches have been properly configured.

Notes: The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 75. Initialize PMAC Application Using CLI

| Step | Procedure | Results |
|--|--|--|
| <p>1. <input type="checkbox"/></p> | <p>TVOE Management Server iLO: Login</p> | <p>1. Log into the management server iLO with Internet Explorer as TVOE admusr user. <code>http://<management_server_iLO_IP></code></p> <p>2. Click on the Remote Console tab and open the Integrated Remote Console on the server.</p> <p>3. Click Yes if the Security Alert displays.</p> |
| <p>2. <input type="checkbox"/></p> | <p>TVOE Application Server iLO: Login</p> | <p>Log into PMAC with admusr credentials.</p> <p>Note: On a TVOE host, if you open the virsh console, for example, <code>\$ sudo /usr/bin/virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or the output is not correct, then there is likely a stuck virsh console command already being run on the TVOE host. Exit out of the virsh console, run <code>ps -ef grep virsh</code>, and then kill the existing process <code>kill -9 <PID></code>. Then execute the <code>virsh console X</code> command. Your console session should now run as expected.</p> <p>Login using virsh and wait until you see the PMAC login prompt.</p> <pre>virsh # list --all Id Name State 13 myTPD running 20 pmacdev7 running virsh # console pmacdev7 Connected to domain pmacdev7 Escape character is ^] CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 pmacdev7 login:</pre> |

Procedure 75. Initialize PMAC Application Using CLI

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|--|--------------------------|-------------|---------------|----------------|-------------|----------|------|---------|--------------------------|---|---------|------|---------|--------------------------|---|--------------|------|---------|--------------------------|---|------------------|------|---------|--------------------------|---|
| <p>3. <input type="checkbox"/></p> | <p>PMAC: Initialize</p> | <p>Initialize the PMAC application with the PMAC profile.</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmacadm applyProfile --fileName=TVOE Profile successfully applied. \$ sudo /usr/TKLC/smac/bin/pmacadm finishProfileConfig Initialization has been started as a background task</pre> <p>Wait for the background task to complete successfully. The command displays IN_PROGRESS for a short time.</p> <p>Run the following command until a COMPLETE or FAILED response is seen similar to the following:</p> <pre>\$ sudo /usr/TKLC/smac/bin/pmaccli getBgTasks 1: Initialize PMAC COMPLETE - PMAC initialized Step 2: of 2 Started: 2012-07-13 08:23:55 running: 29 sinceUpdate: 47 taskRecordNum: 2 Server Identity: Physical Blade Location: Blade Enclosure: Blade Enclosure Bay: Guest VM Location: Host IP: Guest Name: TPD IP: Rack Mount Server: IP: Name:</pre> | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>4. <input type="checkbox"/></p> | <p>PMAC: Perform a system health check</p> | <pre>\$ sudo /usr/TKLC/plat/bin/alarmMgr --alarmStatus</pre> <p>This command should return no output on a healthy system.</p> <pre>\$ sudo /usr/TKLC/smac/bin/sentry status</pre> <p>All processes should be running, displaying output similar to the following:</p> <p><u>PMAC Sentry Status</u></p> <pre>sentryd started: Mon Jul 23 17:50:49 2012 Current activity mode: ACTIVE</pre> <table border="1"> <thead> <tr> <th><u>Process</u></th> <th><u>PID</u></th> <th><u>Status</u></th> <th><u>StartTS</u></th> <th><u>NumR</u></th> </tr> </thead> <tbody> <tr> <td>smacTalk</td> <td>9039</td> <td>running</td> <td>Tue Jul 24 12:50:29 2012</td> <td>2</td> </tr> <tr> <td>smacMon</td> <td>9094</td> <td>running</td> <td>Tue Jul 24 12:50:29 2012</td> <td>2</td> </tr> <tr> <td>hpiPortAudit</td> <td>9137</td> <td>running</td> <td>Tue Jul 24 12:50:29 2012</td> <td>2</td> </tr> <tr> <td>snmpEventHandler</td> <td>9176</td> <td>running</td> <td>Tue Jul 24 12:50:29 2012</td> <td>2</td> </tr> </tbody> </table> <pre>Fri Aug 3 13:16:35 2012 Command Complete.</pre> | <u>Process</u> | <u>PID</u> | <u>Status</u> | <u>StartTS</u> | <u>NumR</u> | smacTalk | 9039 | running | Tue Jul 24 12:50:29 2012 | 2 | smacMon | 9094 | running | Tue Jul 24 12:50:29 2012 | 2 | hpiPortAudit | 9137 | running | Tue Jul 24 12:50:29 2012 | 2 | snmpEventHandler | 9176 | running | Tue Jul 24 12:50:29 2012 | 2 |
| <u>Process</u> | <u>PID</u> | <u>Status</u> | <u>StartTS</u> | <u>NumR</u> | | | | | | | | | | | | | | | | | | | | | | | |
| smacTalk | 9039 | running | Tue Jul 24 12:50:29 2012 | 2 | | | | | | | | | | | | | | | | | | | | | | | |
| smacMon | 9094 | running | Tue Jul 24 12:50:29 2012 | 2 | | | | | | | | | | | | | | | | | | | | | | | |
| hpiPortAudit | 9137 | running | Tue Jul 24 12:50:29 2012 | 2 | | | | | | | | | | | | | | | | | | | | | | | |
| snmpEventHandler | 9176 | running | Tue Jul 24 12:50:29 2012 | 2 | | | | | | | | | | | | | | | | | | | | | | | |
| <p>5. <input type="checkbox"/></p> | <p>Virsh Console: Log out</p> | <p>Exit the virsh console session using Appendix E.2 Exit a Guest Console Session on an iLO.</p> | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>6. <input type="checkbox"/></p> | <p>Management Server iLO: Exit the TVOE console</p> | <pre>\$ logout</pre> | | | | | | | | | | | | | | | | | | | | | | | | | |

9.22.2 Initialize PMAC Application Using the GUI

This procedure initializes the PMAC application and network resources using the GUI.


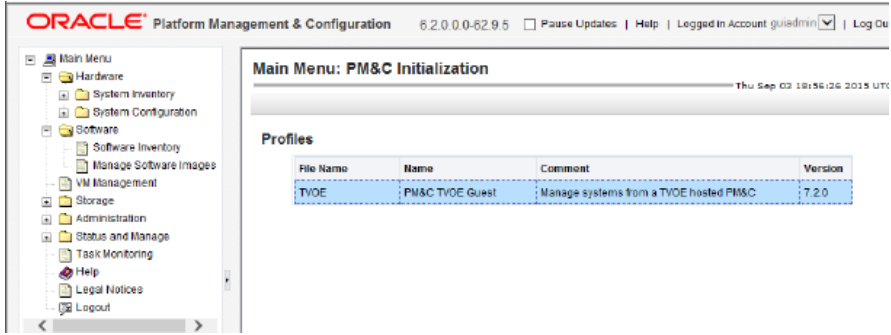
Prerequisites:

- PMAC has been deployed and is not initialized or fully configured.
- Aggregation switches have been properly configured.

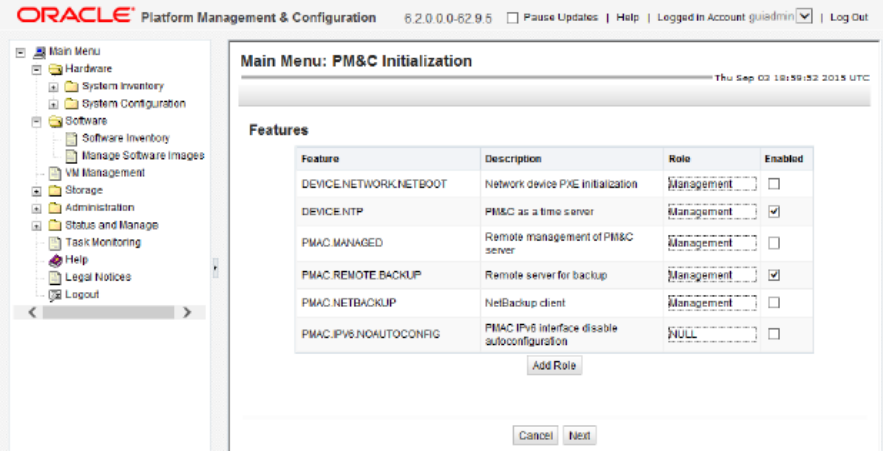
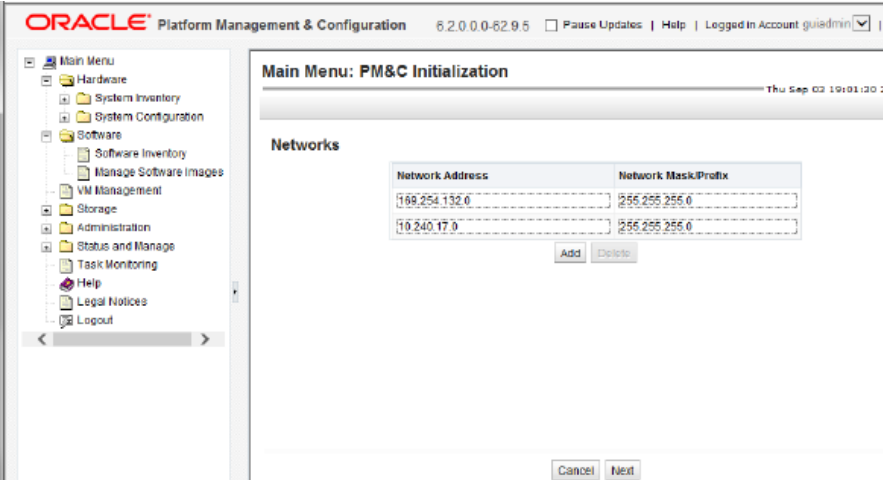
Notes: The installer must know the network and application requirements. The final step configures and restarts the network and the PMAC application; network access is briefly interrupted.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

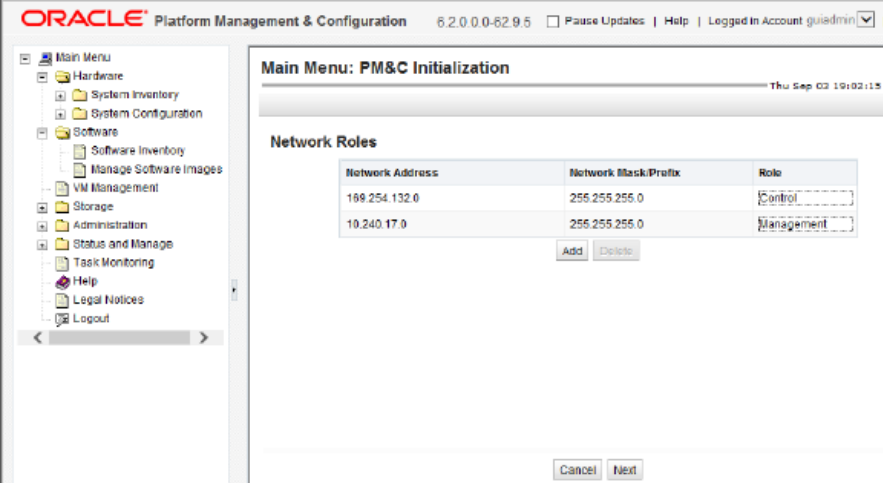
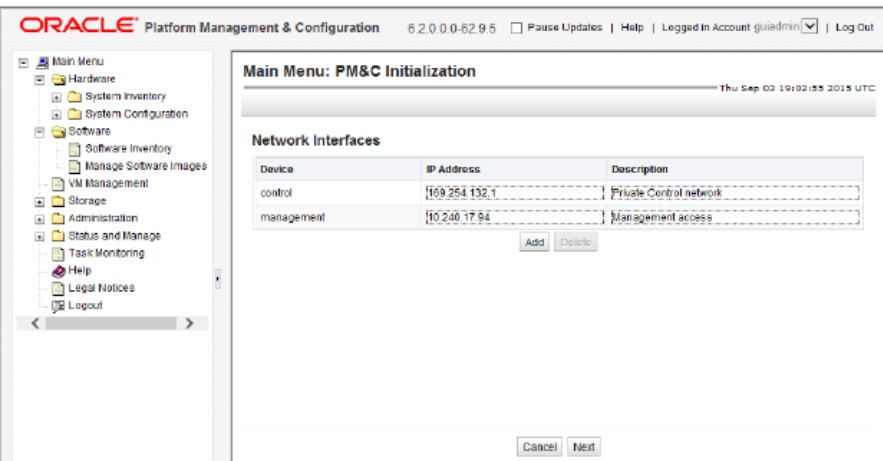
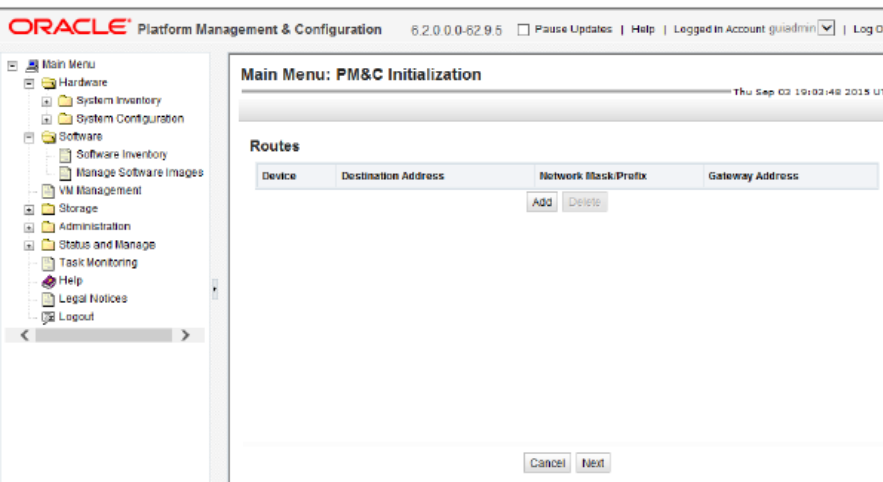
Procedure 76. Initialize PMAC Application Using the GUI

| Step | Procedure | Results |
|--|---|--|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guidadmin user.</p>  <p>Navigate to Administration > PMAC Configuration.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select initialization profile</p> | <p>Select the appropriate PMAC initialization profile.</p>  |

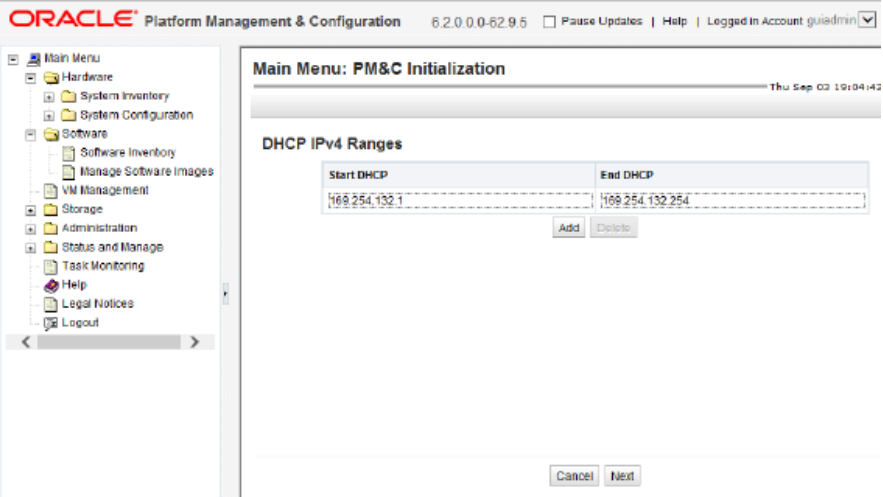
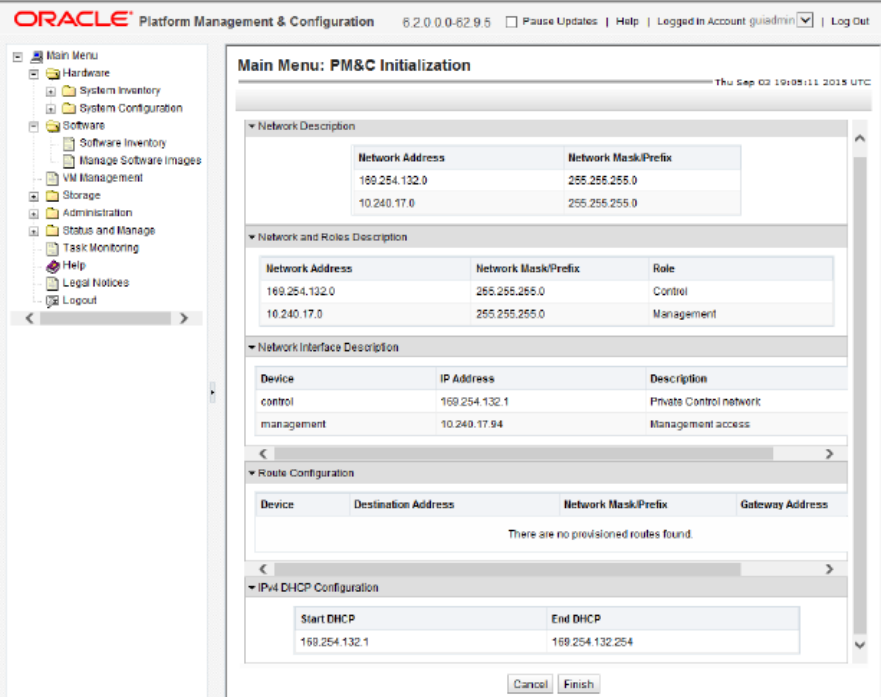

Procedure 76. Initialize PMAC Application Using the GUI

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------------------------------------|---|--|-------------------------------------|---------------------|---------------|---------------|------------------------|-----------------------------------|------------|--------------------------|------------|-----------------------|------------|-------------------------------------|--------------|----------------------------------|------------|--------------------------|--------------------|--------------------------|------------|-------------------------------------|----------------|------------------|------------|--------------------------|------------------------|---|------|--------------------------|
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Select features and roles</p> | <p>Select and enable, appropriate PMAC features and, if required, add new Roles. Click Next.</p>  <table border="1" data-bbox="792 562 1312 766"> <thead> <tr> <th>Feature</th> <th>Description</th> <th>Role</th> <th>Enabled</th> </tr> </thead> <tbody> <tr> <td>DEVICE.NETWORK.NETBOOT</td> <td>Network device PXE initialization</td> <td>Management</td> <td><input type="checkbox"/></td> </tr> <tr> <td>DEVICE.NTP</td> <td>PM&C as a time server</td> <td>Management</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PMAC.MANAGED</td> <td>Remote management of PM&C server</td> <td>Management</td> <td><input type="checkbox"/></td> </tr> <tr> <td>PMAC.REMOTE.BACKUP</td> <td>Remote server for backup</td> <td>Management</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>PMAC.NETBACKUP</td> <td>NetBackup client</td> <td>Management</td> <td><input type="checkbox"/></td> </tr> <tr> <td>PMAC.IPV6.NOAUTOCONFIG</td> <td>PMAC IPv6 interface disable autoconfiguration</td> <td>NULL</td> <td><input type="checkbox"/></td> </tr> </tbody> </table> | Feature | Description | Role | Enabled | DEVICE.NETWORK.NETBOOT | Network device PXE initialization | Management | <input type="checkbox"/> | DEVICE.NTP | PM&C as a time server | Management | <input checked="" type="checkbox"/> | PMAC.MANAGED | Remote management of PM&C server | Management | <input type="checkbox"/> | PMAC.REMOTE.BACKUP | Remote server for backup | Management | <input checked="" type="checkbox"/> | PMAC.NETBACKUP | NetBackup client | Management | <input type="checkbox"/> | PMAC.IPV6.NOAUTOCONFIG | PMAC IPv6 interface disable autoconfiguration | NULL | <input type="checkbox"/> |
| Feature | Description | Role | Enabled | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DEVICE.NETWORK.NETBOOT | Network device PXE initialization | Management | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| DEVICE.NTP | PM&C as a time server | Management | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.MANAGED | Remote management of PM&C server | Management | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.REMOTE.BACKUP | Remote server for backup | Management | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.NETBACKUP | NetBackup client | Management | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| PMAC.IPV6.NOAUTOCONFIG | PMAC IPv6 interface disable autoconfiguration | NULL | <input type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Provision network</p> | <p>Provision the PMAC application networks and click Next.</p>  <table border="1" data-bbox="889 1087 1300 1165"> <thead> <tr> <th>Network Address</th> <th>Network Mask/Prefix</th> </tr> </thead> <tbody> <tr> <td>169.254.132.0</td> <td>255.255.255.0</td> </tr> <tr> <td>10.240.17.0</td> <td>255.255.255.0</td> </tr> </tbody> </table> | Network Address | Network Mask/Prefix | 169.254.132.0 | 255.255.255.0 | 10.240.17.0 | 255.255.255.0 | | | | | | | | | | | | | | | | | | | | | | |
| Network Address | Network Mask/Prefix | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 169.254.132.0 | 255.255.255.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 10.240.17.0 | 255.255.255.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 76. Initialize PMAC Application Using the GUI

| Step | Procedure | Results |
|---|--|--|
| <p>5.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Provision network roles</p> | <p>Provision the PMAC application network roles and click Next.</p>  |
| <p>6.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Provision network interfaces</p> | <p>Provision the PMAC application network interface and click Next.</p>  |
| <p>7.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Provision application routes</p> | <p>Provision the PMAC application routes and click Next.</p>  |

Procedure 76. Initialize PMAC Application Using the GUI

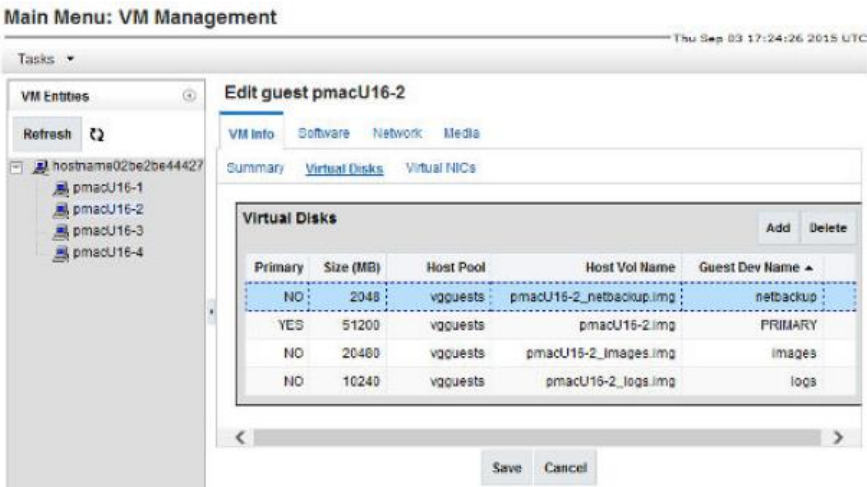
| Step | Procedure | Results |
|--|---|--|
| <p>8.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Provision application DHCP ranges</p> | <p>Provision the PMAC application DHCP ranges and click Next.</p>  |
| <p>9.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Verify</p> | <p>Verify the PMAC application initialization is correct on the Configuration Summary screen and click Finish.</p>  |
| <p>10.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Monitor and verify</p> | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Initialize PMAC background task. A separate task displays for each server.</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |

9.23 Configure PMAC Application Guest NetBackup Virtual Disk

This procedure configures the PMAC application guest NetBackup virtual disk.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 77. Configure PMAC Application Guest NetBackup Virtual Disk

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|---|---|-------------------------|----------------|-----------|---------------|----------------|----|------|----------|-------------------------|-----------|-----|-------|----------|---------------|---------|----|-------|----------|----------------------|--------|----|-------|----------|--------------------|------|
| 1. <input type="checkbox"/> | PMAC GUI: Determine if the PMAC application guest is configured with a NetBackup virtual disk | Navigate to the Virtual Machine Management screen and select the PMAC application guest from the VM Entities list. From the VM Info tab, select the Virtual Disks sub-tab. Determine if the Virtual Disks list contains the NetBackup device. If the NetBackup device exists for the PMAC application guest, then the NetBackup Virtual Disk has already been configure; otherwise, continue to the next step | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. <input type="checkbox"/> | PMAC GUI: Edit the guest to add the NetBackup virtual disk | Click Edit and Add , then type the following data for the new NetBackup virtual disk. <ul style="list-style-type: none"> • Size (MB): 2048 • Host Pool: vgquests • Host Vol Name: <pmacGuestName>_netbackup.img • Guest Dev Name: netbackup <p>Note: The Guest Dev Name must be set to netbackup for the PMAC application to mount the appropriate host device. The <pmacGuestName> variable should be set to this PMAC guest's name to create a unique volume name on the TVOE host of the PMAC.</p> | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. <input type="checkbox"/> | PMAC GUI: Verify | Verify the new NetBackup virtual disk data and click Save .  <p>The screenshot shows the 'Edit guest pmacU16-2' window with the 'Virtual Disks' tab selected. The table below is a representation of the data shown in the screenshot:</p> <table border="1"> <thead> <tr> <th>Primary</th> <th>Size (MB)</th> <th>Host Pool</th> <th>Host Vol Name</th> <th>Guest Dev Name</th> </tr> </thead> <tbody> <tr> <td>NO</td> <td>2048</td> <td>vgquests</td> <td>pmacU16-2_netbackup.img</td> <td>netbackup</td> </tr> <tr> <td>YES</td> <td>51200</td> <td>vgquests</td> <td>pmacU16-2.img</td> <td>PRIMARY</td> </tr> <tr> <td>NO</td> <td>20480</td> <td>vgquests</td> <td>pmacU16-2_images.img</td> <td>images</td> </tr> <tr> <td>NO</td> <td>10240</td> <td>vgquests</td> <td>pmacU16-2_logs.img</td> <td>logs</td> </tr> </tbody> </table> | Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | NO | 2048 | vgquests | pmacU16-2_netbackup.img | netbackup | YES | 51200 | vgquests | pmacU16-2.img | PRIMARY | NO | 20480 | vgquests | pmacU16-2_images.img | images | NO | 10240 | vgquests | pmacU16-2_logs.img | logs |
| Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | | | | | | | | | | | | | | | | | | | | | | | |
| NO | 2048 | vgquests | pmacU16-2_netbackup.img | netbackup | | | | | | | | | | | | | | | | | | | | | | | |
| YES | 51200 | vgquests | pmacU16-2.img | PRIMARY | | | | | | | | | | | | | | | | | | | | | | | |
| NO | 20480 | vgquests | pmacU16-2_images.img | images | | | | | | | | | | | | | | | | | | | | | | | |
| NO | 10240 | vgquests | pmacU16-2_logs.img | logs | | | | | | | | | | | | | | | | | | | | | | | |
| 4. <input type="checkbox"/> | PMAC GUI: Confirm the PMAC application guest list | Click OK on the confirmation screen. | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 77. Configure PMAC Application Guest NetBackup Virtual Disk

| Step | Procedure | Results |
|--------------------------------|--|--|
| 5. <input type="checkbox"/> | PMAC GUI: Monitor and verify | Navigate to Main Menu > Task Monitoring to monitor the progress of the Guest Edit background task. When the task is complete, the text changes to green and the Progress column indicates 100%. |
| 6. <input type="checkbox"/> | TVOE Management Server iLO: Shut down | Shut down the PMAC application guest. Note: To configure the PMAC application with the new NetBackup virtual disk the PMAC application guest needs to be shut down and restarted. Refer to <i>PMAC Incremental Upgrade</i> , Release 6.6, E91174-01, Appendix O, Shutdown PMAC 5.5 or Later Guest. |
| 7. <input type="checkbox"/> | TVOE Management Server iLO: Start the PMAC application guest | Using virsh utility on TVOE host of the PMAC guest, start the PMAC guest. Query the list of guests until the PMAC guest is running . \$ sudo /usr/bin/virsh <pre>virsh # list --all Id Name State -- - 20 pmacU14-1 shut off virsh # start pmacU14-1 Domain pmacU14-1 started virsh # list --all Id Name State -- - 20 pmacU14-1 running</pre> |

9.24 PMAC Guest Migrate NetBackup Client to New File System

If the NetBackup client software was installed on a PMAC application guest before the NetBackup virtual disk required for a PMAC deploys with NetBackup, execute 9.23 Configure PMAC Application Guest NetBackup Virtual Disk. This creates a new NetBackup virtual disk for the PMAC guest. The PMAC guest is shut down and restarted. The content of the **/usr/opensv** directory is moved to the new NetBackup virtual disk, and mounted at **/usr/opensv**.


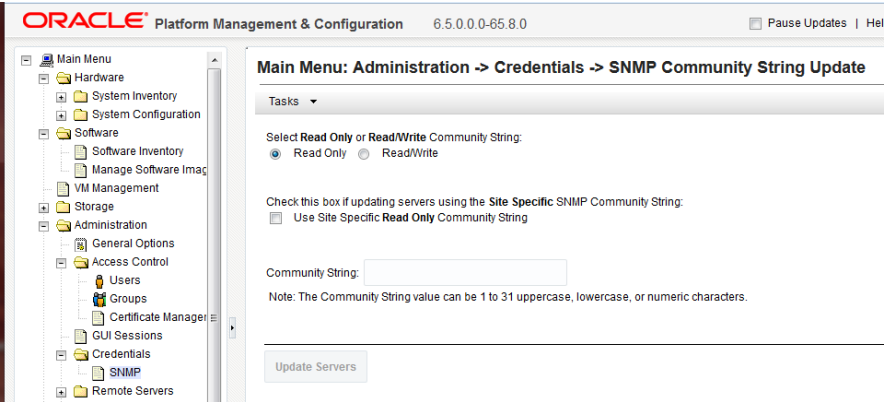
9.25 Update the TVOE Host SNMP Community String from the GUI

This procedure uses the PMAC GUI to update the read only or read/write SNMP community string on all TVOE hosting servers and the PMAC guest TPD, which are known to the PMAC control network.


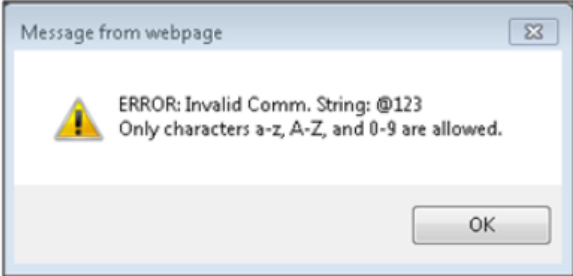
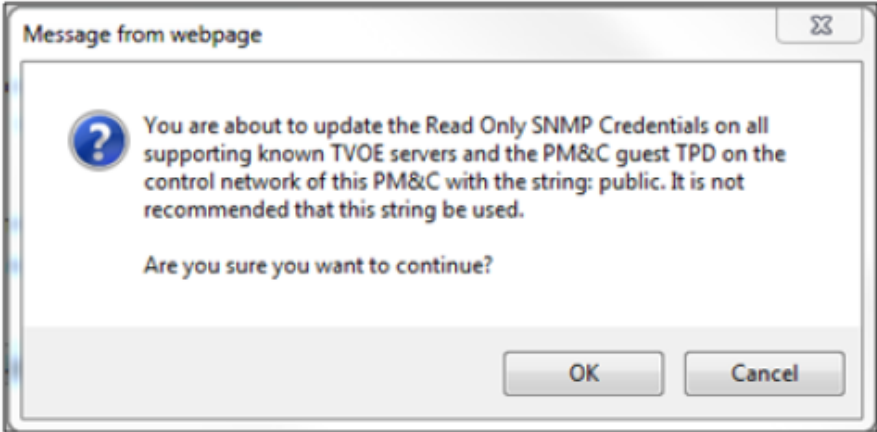
Prerequisite: You must be logged in as the Admin user to access this page.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

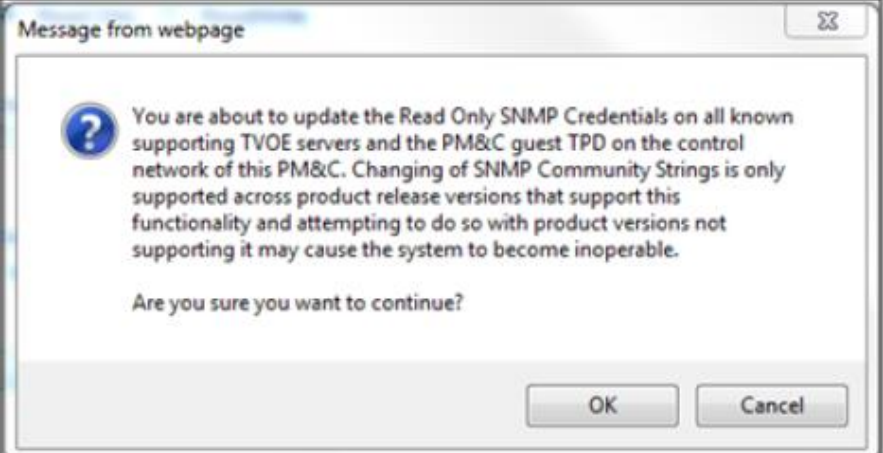
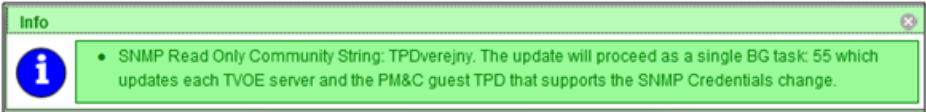
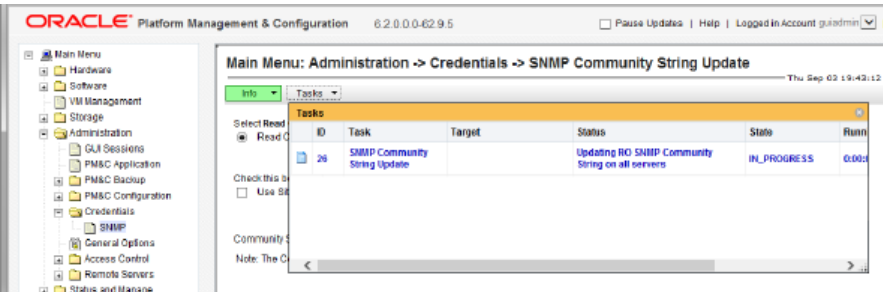
Procedure 78. Update the TVOE Host SNMP Community String from the GUI

| Step | Procedure | Results |
|------------------------------------|---------------------------------------|--|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guidadmin user.</p>  |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Configure</p> | <ol style="list-style-type: none"> Navigate to Administration > Credentials > SNMP. Select the Read Only or Read/Write option depending on which SNMP Community String needs to be updated. If this is the first time the SNMP Community Strings have been updated for this PMAC, then leave the Use Site Specific checkbox unmarked and type a new Read Only Community String into the Community String textbox. <p>Note: The string may only contain 1 to 31 characters in the set a-z, A-Z, and 0-9.</p> <p>If you want to update one or more servers hosting the TVOE application after the Read Only and/or Read/Write Community String has already been updated, then select the Use Site Specific checkbox. This disables the Community String textbox and enables the Update Servers button because the string to be used is the one stored in the PMAC database.</p>  |

Procedure 78. Update the TVOE Host SNMP Community String from the GUI

| Step | Procedure | Results |
|---|------------------------|--|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI</p> | <p>Click Update Servers.</p> <p>The following error or warning messages may display depending on the Community String entered:</p> <ul style="list-style-type: none"> Invalid string length (over 31 characters)  <ul style="list-style-type: none"> Invalid characters (must be a-z, A-Z, 0-9)  <ul style="list-style-type: none"> Use of non-recommended Community String (any mixed case combination of public, private, password, or snmp-trap).  <p>These whole words are not recommended as a standard Community String, but the user is allowed to override the controls and allow the string to be set.</p> <ul style="list-style-type: none"> Valid Community String general warning. |

Procedure 78. Update the TVOE Host SNMP Community String from the GUI

| Step | Procedure | Results |
|------------------------------------|--|---|
| | |  <p>This general warning is always displayed after the Community String validation is performed to make sure the user is aware that changing these TVOE host Community Strings can cause their system to become inoperable if other components are not changed to reflect what is entered here.</p> <p>Click OK.</p> <p>Note: When this operation is initiated, all supporting TVOE hosting servers and the PMAC guest TPD on the PMAC control network update. All those servers that match the existing Site Specific Community String are not updated again until the string name is changed.</p> |
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Monitor the status</p> | <p>Click Info to access the status and watch for a successful or failed update.</p>  <p>Click Tasks located on the toolbar to monitor the progress.</p>  <p>Or navigate to Main Menu > Task Monitoring screen.</p> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |
| <p>5. <input type="checkbox"/></p> | <p>Validate the task</p> | <p>If the update needs to be validated, the user can type the pmaccli <code>getCommStrStatus</code> command at a SSH terminal connection to the PMAC to display the status of the Community Strings on all servers on the PMAC control network.</p> <p>Execution loops over all known servers on the PMAC control network and</p> |

Procedure 78. Update the TVOE Host SNMP Community String from the GUI

| Step | Procedure | Results |
|------|-----------|---|
| | | <p>attempts to retrieve the Read Only and Read/Write Community String. It displays the IPv4 and IPv6 for each server, the TPD release, the Application name and version, whether the servers supports the update functionality, and the status of the Community Strings for that server. All servers whose TPD instance is greater than 6.5.0_82.4.0 are queried. It uses the values set in the PMAC database to determine the status of each Community String. The status can be any of the following:</p> <ul style="list-style-type: none"> • Query Failed - Unable to retrieve the Read Only and Read/Write Community Strings from a given server. • Site Specific - Matches the current (the non-default) Read Only or Read/Write Community String stored in the PMAC database. • Default - Matches the default (non-editable) Read Only or Read/Write Community String stored in the PMAC database. • Unknown - Was able to retrieve the Read Only or Read/Write Community String but it does not match what is maintained in the PMAC database. Usually indicates the Community String was updated manually from an interface other than the PMAC. • Not Applicable - This indicates the server does not support the Update functionality and therefore the status cannot be determined. It is assumed this server matches the default values since they cannot be updated. Usually the server release is an older TPD and Application or a TVOE of < 2.5.0-82.4.0. <p>The output of the command includes Server Update Supported with a value indicating if the Update is actually supported or not. The possible values for support are:</p> <ul style="list-style-type: none"> • Supported - This indicates the TPD release is >= 6.5.0_82.4.0 and the Application name is TVOE or PMAC. • Supported for Query Only - This indicates the TPD release is >= 6.5.0_82.4.0 and the Application name is unknown or something other than TVOE or PMAC. The Community Strings will not be updated via the PMAC, but they can be queried from this command or the <code>getHostCommStr</code> command. • Not Supported - This indicates the TPD release is < 6.5.0_82.4.0 and cannot be queried. In this case the Community String is set to the default values and the status is indicated as Not Applicable. <p>Example output:</p> |

Procedure 78. Update the TVOE Host SNMP Community String from the GUI

| Step | Procedure | Results |
|------|-----------|--|
| | | <pre> dnaccli getCommStrStatus SNMP Credentials Status Info: ----- Server IP Address (IPv4 - IPv6) : 169.254.131.6 - fe80::b699:baff:fea8:b860 Server Release Info (Host - App): TPD: 6.0.0-80.28.1 - Unknown: Unknown Server Update Supported : Not Supported SNMP Read Only Community String : TPDverejny - Status: Not Applicable SNMP Read Write Community String: TPDsoukromy - Status: Not Applicable Server IP Address (IPv4 - IPv6) : 169.254.131.7 - fe80::1ccl:deff:fe75:df00 Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0 Server Update Supported : Supported SNMP Read Only Community String : neustestrol - Status: Site Specific SNMP Read Write Community String: neustrwl - Status: Site Specific Server IP Address (IPv4 - IPv6) : 169.254.131.12 - fe80::5054:ff:feee:850 Server Release Info (Host - App): TPD: 6.0.0-80.20.0 - Unknown: Unknown Server Update Supported : Not Supported SNMP Read Only Community String : TPDverejny - Status: Not Applicable SNMP Read Write Community String: TPDsoukromy - Status: Not Applicable Server IP Address (IPv4 - IPv6) : 169.254.131.14 - fe80::5054:ff:fe07:ea61 Server Release Info (Host - App): TPD: 5.0.0-72.44.0 - Unknown: Unknown Server Update Supported : Not Supported SNMP Read Only Community String : TPDverejny - Status: Not Applicable SNMP Read Write Community String: TPDsoukromy - Status: Not Applicable Server IP Address (IPv4 - IPv6) : 169.254.131.8 - fe80::1ccl:deff:fe75:fcc0 Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0 Server Update Supported : Supported SNMP Read Only Community String : neustestrol - Status: Site Specific SNMP Read Write Community String: neustrwl - Status: Site Specific Server IP Address (IPv4 - IPv6) : 169.254.131.5 - fe80::2e76:8aff:fe50:3974 Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0 Server Update Supported : Supported SNMP Read Only Community String : neustestrol - Status: Site Specific SNMP Read Write Community String: neustrwl - Status: Site Specific Server IP Address (IPv4 - IPv6) : 169.254.131.2 - fe80::3ed9:2bff:fef6:3e38 Server Release Info (Host - App): TPD: 6.5.0-82.4.0 - TVOE: 2.5.0_82.4.0 Server Update Supported : Supported SNMP Read Only Community String : testro - Status: Unknown SNMP Read Write Community String: neustrwl - Status: Site Specific </pre> |

9.26 Configure PMAC Application Guest Isoimages Virtual Disk

This procedure expands the PMAC temporary area for importing software images using sftp in cases where PMAC already exists and larger ISO images need to be imported. The preferred method is to designate the extra space during PMAC deployment, refer to 9.3 Deploy PMAC Guest.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 79. Configure PMAC Application Guest Isoimages Virtual Disk

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|---|--|-------------------------|----------------|-----|--------|--|-----|--------|---------|-----------|-----------|---------------|----------------|--|--|-----|-------|----------|---------------|---------|--|--|----|-------|----------|--------------------|------|--|--|----|-------|----------|----------------------|--------|--|--|----|-------|----------|-------------------------|-----------|--|--|
| 1. <input type="checkbox"/> | PMAC GUI: Determine if the PMAC application guest is configured with a isoimages virtual disk | Navigate to the Virtual Machine Management screen and select the PMAC application guest from the VM Entities list. From the VM Info tab, select the Virtual Disks sub-tab. Determine if the Virtual Disks list contains the isoimages device. If the isoimages device exists for the PMAC application guest, then the isoimages Virtual Disk has already been configure; otherwise, continue to the next step | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. <input type="checkbox"/> | PMAC GUI: Edit the guest to add the isoimages virtual disk | Click Edit and Add , then type the following data for the new NetBackup virtual disk. <ul style="list-style-type: none"> • Size (MB): 2048 • Host Pool: vgquests • Host Vol Name: <pmacGuestName>_isoimages.img • Guest Dev Name: isoimages <p>Note: The Guest Dev Name must be set to isoimages for the PMAC application to mount the appropriate host device. The <pmacGuestName> variable should be set to this PMAC guest's name to create a unique volume name on the TVOE host of the PMAC.</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. <input type="checkbox"/> | PMAC GUI: Verify | Verify the new isoimages virtual disk data and click Save . <div style="border: 1px solid gray; padding: 5px;"> <p>Main Menu: VM Management Thu Sep 17 19:16:50 2015 U</p> <p>Tasks ▾</p> <div style="display: flex;"> <div style="flex: 1;"> <p>VM Entities</p> <p>Refresh ↻</p> <ul style="list-style-type: none"> hostname02be2be44427 <ul style="list-style-type: none"> pmacU16-1 pmacU16-2 pmacU16-3 pmacU16-4 hostname5199ee5b4c5d hostname7b02759a2e0c </div> <div style="flex: 2;"> <p>Edit guest pmacU16-4</p> <p>VM Info Software Network Media</p> <p>Summary Virtual Disks Virtual NICs</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th colspan="5">Virtual Disks</th> <th style="text-align: right;">Add</th> <th style="text-align: right;">Delete</th> </tr> <tr> <th>Primary</th> <th>Size (MB)</th> <th>Host Pool</th> <th>Host Vol Name</th> <th>Guest Dev Name</th> <th colspan="2"></th> </tr> </thead> <tbody> <tr> <td>YES</td> <td>51200</td> <td>vgquests</td> <td>pmacU16-4.img</td> <td>PRIMARY</td> <td colspan="2"></td> </tr> <tr> <td>NO</td> <td>10240</td> <td>vgquests</td> <td>pmacU16-4_logs.img</td> <td>logs</td> <td colspan="2"></td> </tr> <tr> <td>NO</td> <td>20480</td> <td>vgquests</td> <td>pmacU16-4_images.img</td> <td>images</td> <td colspan="2"></td> </tr> <tr style="border: 2px dashed blue;"> <td>NO</td> <td>20480</td> <td>vgquests</td> <td>pmacU16-4_isoimages.img</td> <td>isoimages</td> <td colspan="2"></td> </tr> </tbody> </table> <p style="text-align: right; margin-top: 10px;">Save Cancel</p> </div> </div> </div> | Virtual Disks | | | | | Add | Delete | Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | | | YES | 51200 | vgquests | pmacU16-4.img | PRIMARY | | | NO | 10240 | vgquests | pmacU16-4_logs.img | logs | | | NO | 20480 | vgquests | pmacU16-4_images.img | images | | | NO | 20480 | vgquests | pmacU16-4_isoimages.img | isoimages | | |
| Virtual Disks | | | | | Add | Delete | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| YES | 51200 | vgquests | pmacU16-4.img | PRIMARY | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NO | 10240 | vgquests | pmacU16-4_logs.img | logs | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NO | 20480 | vgquests | pmacU16-4_images.img | images | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NO | 20480 | vgquests | pmacU16-4_isoimages.img | isoimages | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 79. Configure PMAC Application Guest Isoimages Virtual Disk

| Step | Procedure | Results |
|--------------------------------|--|--|
| 4. <input type="checkbox"/> | PMAC GUI: Confirm the PMAC application guest list | Click OK on the confirmation screen. |
| 5. <input type="checkbox"/> | PMAC GUI: Monitor and verify | Navigate to Main Menu > Task Monitoring to monitor the progress of the Guest Edit background task. When the task is complete, the text changes to green and the Progress column indicates 100%. |
| 6. <input type="checkbox"/> | TVOE Management Server iLO: Shut down | Shut down the PMAC application guest. Note: To configure the PMAC application with the new isoimages virtual disk the PMAC application guest needs to be shut down and restarted. Refer to <i>PMAC Incremental Upgrade</i> , Release 6.6, E91174-01, Appendix O, Shutdown PMAC 5.5 or Later Guest. |
| 7. <input type="checkbox"/> | TVOE Management Server iLO: Start the PMAC application guest | Using virsh utility on TVOE host of the PMAC guest, start the PMAC guest. Query the list of guests until the PMAC guest is running . \$ sudo /usr/bin/virsh <pre>virsh # list --all Id Name State 20 pmacU14-1 shut off virsh # start pmacU14-1 Domain pmacU14-1 started virsh # list --all Id Name State 20 pmacU14-1 running</pre> |

9.27 Certificate Management

9.27.1 Generate a New Certificate Signing Request


This procedure generates a new self-signed HTTPS certificate and a Certificate Signing Request to be submitted to the customer’s Certificate Authority. The CA provides a signed certificate that can be used to replace the self-signed certificate using the procedure Update an HTTPS Certificate.

Use this procedure if the customer does not already have an HTTPS certificate to install. Such a certificate may have been generated by a previous use of this procedure or by using the customer's own procedure. If the customer already has a certificate to install, use Import an HTTPS Certificate or Update an HTTPS Certificate instead.


Prerequisite: 9.30 Configure PMAC Domain Name System

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 80. Generate a New Certificate Signing Request

| Step | Results | | | | | | | | | | |
|--|--|--|--------------------|--|--------------------|-------------|-------------------|----------------|--|-------------|--|
| <p>1. <input type="checkbox"/></p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  | | | | | | | | | | |
| <p>2. <input type="checkbox"/></p> | <p>1. Navigate to Administration > Access Control > Certificate Management. 2. Click Create CSR.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management Fri Sep 04 16:50:10 2015 UTC</p> <p>Info ▾</p> <table border="1" data-bbox="310 1119 1154 1243"> <thead> <tr> <th>Certificate Name</th> <th>Certificate Type</th> <th>Certificate Subject</th> <th>Certificate Issuer</th> <th>Valid Dates</th> </tr> </thead> <tbody> <tr> <td>*.labs.oracle.com</td> <td>HTTPS Wildcard</td> <td>Common Name: *.labs.oracle.com Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 4, 2015, 4:49 pm To: October 4, 2015, 4:49 pm</td> </tr> </tbody> </table> <p>Establish SSO Zone Create CSR Import Delete Report</p> | Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | *.labs.oracle.com | HTTPS Wildcard | Common Name: *.labs.oracle.com Organization: Oracle | Self-Signed | From: September 4, 2015, 4:49 pm To: October 4, 2015, 4:49 pm |
| Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | | | | | | | |
| *.labs.oracle.com | HTTPS Wildcard | Common Name: *.labs.oracle.com Organization: Oracle | Self-Signed | From: September 4, 2015, 4:49 pm To: October 4, 2015, 4:49 pm | | | | | | | |

Procedure 80. Generate a New Certificate Signing Request

| Step | Results |
|--|--|
| <p>3. <input type="checkbox"/></p> | <p>Edit fields to describe the system for which the new certificate will be generated. All fields are required.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management [Create CSR]</p> <p style="text-align: right;">Fri Sep 04 16:54:45 2015 UT</p>  <p>The Common Name determines whether the new certificate applies only to this PMAC host (for example, pmac1.office.company.com) or to any host in the same domain (for example, *.office.company.com). Use the host-specific option unless there are other hosts in the same domain sharing a single certificate.</p> <p>The Common Name only offer names for which no certificate is already present on this PMAC. To replace an existing certificate, first delete it as instructed in 9.27.4 Delete an HTTPS Certificate.</p> |
| <p>4. <input type="checkbox"/></p> | <p>Click Generate CSR.</p> <p>This creates and installs a new (self-signed) HTTPS certificate in PMAC and writes the related Certificate Signing Request to a file. This file is available immediately using the Status and Manage > Files screen (refer to 9.27.2 Update an HTTPS Certificate).</p> <p>Because a new self-signed certificate is in use now, the user needs to re-establish the GUI session and accept the certificate.</p> |

9.27.2 Update an HTTPS Certificate


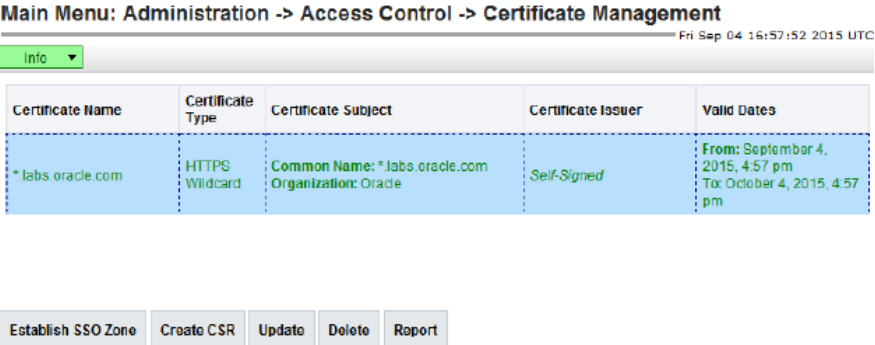
This procedure replaces a self-signed certificate generated by PMAC with a CA-signed certificate provided by the customer's Certificate Authority.

Prerequisites:

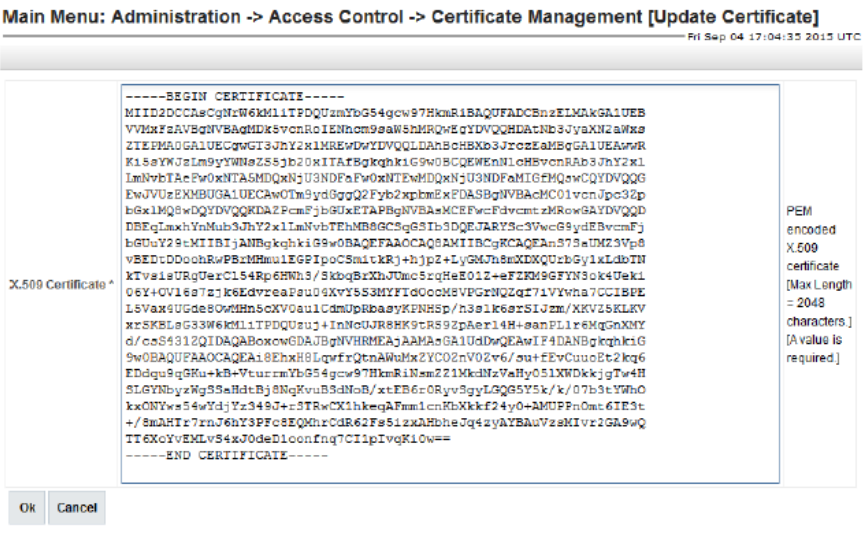
- 9.27.1 Generate a New Certificate Signing Request has been performed to generate a new self-signed certificate and CSR
- The CSR has been submitted to a Certificate Authority
- The CA has provided a signed certificate

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 81. Update an HTTPS Certificate

| Step | Results |
|--|---|
| <p>1. <input type="checkbox"/></p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  |
| <p>2. <input type="checkbox"/></p> | <ol style="list-style-type: none"> 1. Navigate to Administration > Access Control > Certificate Management. 2. Select the certificate to update. 3. Click Update.  |

Procedure 81. Update an HTTPS Certificate

| Step | Results |
|------|--|
| |  |
| 4. | <p>Click OK.</p> <p>The PMAC web server restarts immediately to put the updated certificate into effect. If the signing CA is not known to the browser or the PMAC was not accessed by DNS name, the user has to re-establish the GUI session and accept the new certificate.</p> <p>Users are now able to access the PMAC GUI without having to acknowledge and accept the server's certificate if the following conditions are met:</p> <ul style="list-style-type: none"> The PMAC is accessed by DNS name, not by IP address. This requires either a customer-provided DNS server or configuration of the PMAC host name in the client PC's hosts file. The browser recognizes the CA's signature on the certificate. This requires the certificate be signed by a Certificate Authority known to the browser. Browsers are shipped with well-known CAs already installed, but certificates for additional CAs, such as customer-operated CAs, can be installed manually. |

9.27.3 Import an HTTPS Certificate

This procedure install a certificate and private key provided by the customer. If the key is encrypted, the customer's passphrase for the key must also be provided.

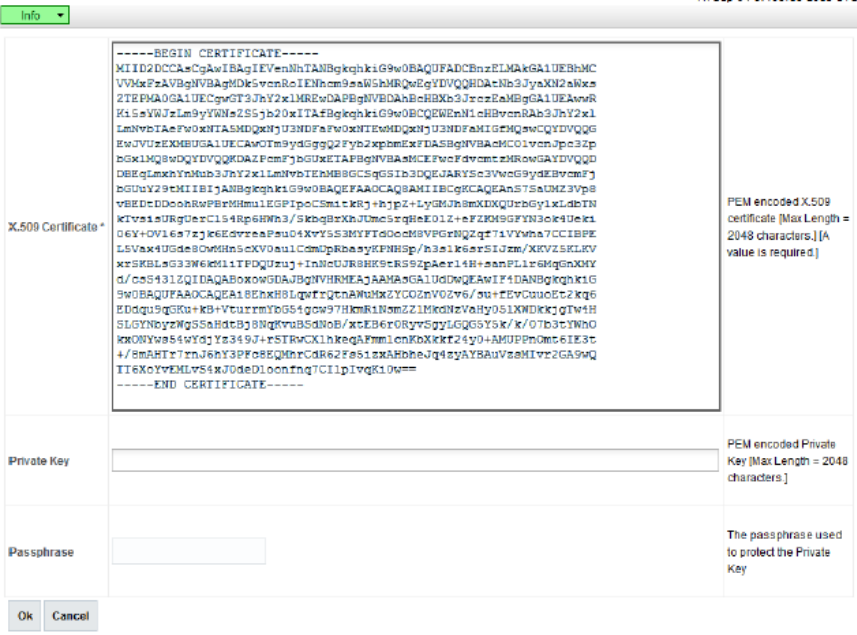
Note: The customer's passphrase is used only once to decrypt the customer's private key. The key is then re-encrypted by PMAC using its own passphrase. The customer's passphrase is not retained by PMAC.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

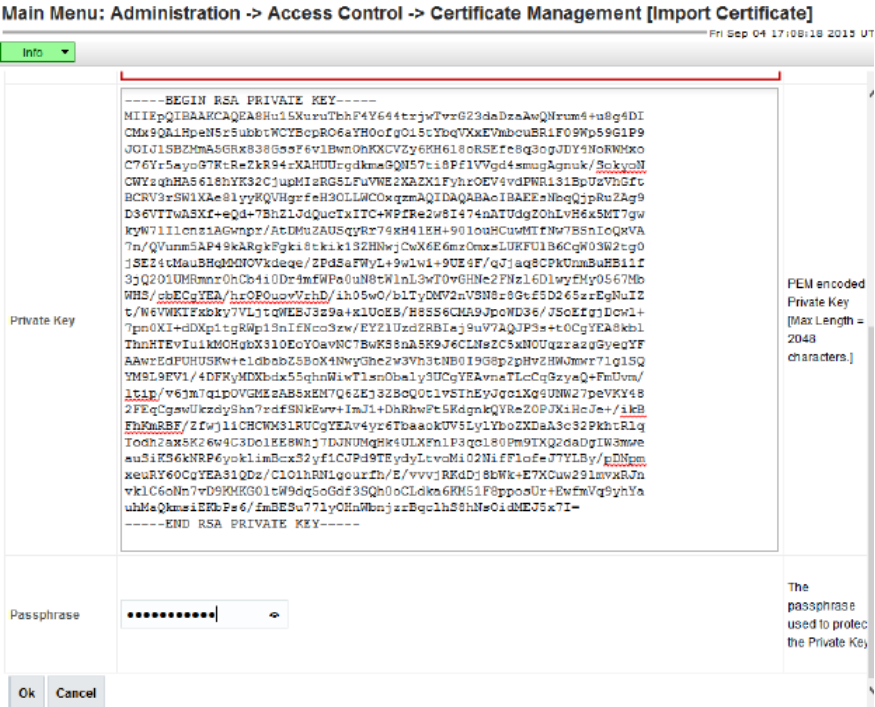
Procedure 82. Import an HTTPS Certificate

| Step | Results |
|---|--|
| <p>1.</p> <p><input type="checkbox"/></p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  |
| <p>2.</p> <p><input type="checkbox"/></p> | <p>1. Navigate to Administration > Access Control > Certificate Management.</p> <p>2. Click Import.</p>  |

Procedure 82. Import an HTTPS Certificate

| Step | Results |
|------------------------------------|---|
| <p>3. <input type="checkbox"/></p> | <p>1. Using an ASCII text editor on the PC, open the signed certificate provided by the Certificate Authority.</p> <p>2. Copy the certificate from the editor to the X.509 Certificate field on the PMAC screen.</p> <p>Include the BEGIN and END lines and everything between:</p> <pre>-----BEGIN CERTIFICATE----- <encoded certificate data> -----END CERTIFICATE-----</pre> <p>Main Menu: Administration -> Access Control -> Certificate Management [Import Certificate]</p>  <p>The screenshot shows the 'Import Certificate' form with the following fields:</p> <ul style="list-style-type: none"> X.509 Certificate: Contains a long PEM-encoded certificate starting with '-----BEGIN CERTIFICATE-----' and ending with '-----END CERTIFICATE-----'. A tooltip indicates: 'PEM encoded X.509 certificate [Max Length = 2048 characters.] [A value is required.]' Private Key: An empty text input field. A tooltip indicates: 'PEM encoded Private Key [Max Length = 2048 characters.]' Passphrase: An empty text input field. A tooltip indicates: 'The passphrase used to protect the Private Key' <p>Buttons: <input type="button" value="Ok"/> <input type="button" value="Cancel"/></p> |

Procedure 82. Import an HTTPS Certificate


| Step | Results |
|---|---|
| <p>4.</p> <p><input type="checkbox"/></p> | <p>1. Using an ASCII text editor on the PC, open the private key file.</p> <p>2. Copy the private key from the editor to the Private Key field on the PMAC screen.</p> <p>Include the BEGIN and END lines and everything between:</p> <pre>-----BEGIN RSA PRIVATE KEY----- <encoded key data> -----END RSA PRIVATE KEY-----</pre> <p>3. If the private key is encrypted, type or paste the passphrase into the Passphrase field.</p>  <p>The screenshot shows the 'Certificate Management [Import Certificate]' page. The 'Private Key' field contains the following text:</p> <pre>-----BEGIN RSA PRIVATE KEY----- MIIEpQIBAAKCAQEA8Hu15XuruTbhP4Y644trjwTvrG23daDzaAeQNrmm4+u8g4DI CMK9QALHpeN5z5ubbtWCTopRO6aYHOcFgO1StYbqVXEVmbouBR1FO9Wp59G1P9 JOI1J1SB2MmASGRx838GoeFev1BwnOnKCKCVZy6KH618oRSEfcbg3ogJDY4NoRNMxk C76Yr5ayo9TRtReZkR94zXAHUUCgdKmaGQh57ti8PF1V7Vgd4smugAgnuK/BckyoM CWYzqhHAs618hYK32C3upMIzRGSLFuVWE2XAZX1FyhrOEV9vdPWR131BpUzVhGfC BCRV3rSW1Xae81yyKQVHgrfeH3OLLWCoxqzmAQIDQAQABAcIBAFEEsNbcQjPrRu2Ag9 D3EVTWASXf+eQd+7BhZLJdQuoTIXC+WFIRE2w8I474nATUJdZOhLvH6x5MT7gw kyW711lonz1AGwnpr/AtDMuZAUSqyRr74xH41EH+901ouHCuMfITNv7B8NLoQKVA 7n/QVum5AP49kARgkFgki8tkk13ZHNnjCwX6E6mzOmzSLURF1B6CgW03W2tg0 jSE24tMaubHq0GVOVkdqde/2PdSaFwYl+9w1w1+9UE4F/qJaq8CPkUmBuHB11f 3jQ2O1UMRmnrOhCb4i0Dr4mFWPa0uN8tW1nL3wT0vGHNe2PNzL6D1wyfM0567Mb WHS/cbECcYEA/hzOF0uqvVchD/ih05w0/blTyDMV2nVSN8r8GtE5D265zrEgNuIZ t/W6VWKIFxbky7VLjtqWEEJ3z9a+xlUoEB/H8SS6CMA9JpoWD36/JSoEfgjDov1+ 7pnoXI+dDXp1tg8Wp13nIFnc03zw/EYZ1Uzd2RBIej9uV7AQJP3e+t0CgYEA8kbl ThnHTEvIu1MMCHqbX310EoY0avNC7BwKS8nA5K9J6CLNeZC5xNOUqzrzazGyeoYF AAwrEdFHHUSKw+clDbobZ5B0K4NvyGhe2w3Vh3tNB019G8p2pHV2HM0mr71q1SQ YMSL9EV1/4DFKyMDXbdx55qhnWiwT1snObelY3UCgYEAvnaTLcCg8zyeQ+FmUvm/ 1t1p/v6jM7q1pOVGMEzAS8xEM7Q6ZEj3Z8oQ0clvStInEyJqolXq6UNW27peVKY48 2FEcGawUkzdyShn7rdfSNkEwv+ImJ1+DhRhwPt5RdgnkQVReZOPJX1HoJe+/ikB EhNmBBE/2fwj11CHCWMSLRUCgYEA4yz6TbaokUV5Ly1Ybo2XDA3c32Pkh:Rlq Todh2am5K26w4C3Do1EE8Whj7DUNUMqHk4ULXFn1F3qo180Pm9TXQ2daDgIW3mwe au5iR56kNRf6yoklimBcx32yf1CJpD9TEydyLtwMi02NiFFloFeJ7YLYb/pdNppm xeuRY60CgYEA31QDz/ClO1hRNlqourTh/E/vvvjRfDdJ8bWk+E7XCuw291mvxR7a vkl6e0Nm7vD9MKG01tW9dq5oGdf3SQh0cLlaka6RM51F8ppo5Ur+EwfmVq9yhYa uhMeQkmsiEhBf6/4mBESu77LyCHnWbnjzrBqqlh86hNeOidMEJ5x7I- -----END RSA PRIVATE KEY-----</pre> <p>The 'Passphrase' field is empty. The interface includes 'Ok' and 'Cancel' buttons.</p> |
| <p>5.</p> <p><input type="checkbox"/></p> | <p>Click OK.</p> <p>The PMAC web server restarts immediately to put the updated certificate into effect. If the signing CA is not known to the browser or the PMAC was not accessed by DNS name, the user has to re-establish the GUI session and accept the new certificate.</p> <p>Users are now able to access the PMAC GUI without having to acknowledge and accept the server's certificate if the following conditions are met:</p> <ul style="list-style-type: none"> • The PMAC is accessed by DNS name, not by IP address. This requires either a customer-provided DNS server or configuration of the PMAC host name in the client PC's hosts file. • The browser recognizes the CA's signature on the certificate. This requires the certificate be signed by a Certificate Authority known to the browser. Browsers are shipped with well-known CAs already installed, but certificates for additional CAs, such as customer-operated CAs, can be installed manually. |

9.27.4 Delete an HTTPS Certificate

This procedure removes a certificate from PMAC. PMAC then reverts to using the default HTTPS certificate. This requires the user to acknowledge and accept the certificate when accessing the PMAC GUI.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 83. Delete an HTTPS Certificate

| Step | Results | | | | | | | | | | |
|------------------------------------|---|---|--------------------|--|--------------------|-------------|------------------|----------------|---|-------------|--|
| <p>1. <input type="checkbox"/></p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  | | | | | | | | | | |
| <p>2. <input type="checkbox"/></p> | <ol style="list-style-type: none"> 1. Navigate to Administration > Access Control > Certificate Management. 2. Select the certificate to delete. 3. Click Delete. <p>Main Menu: Administration -> Access Control -> Certificate Management Fri Sep 04 16:57:52 2015 UTC</p> <p>Info ▾</p> <table border="1" data-bbox="305 1369 1166 1501"> <thead> <tr> <th>Certificate Name</th> <th>Certificate Type</th> <th>Certificate Subject</th> <th>Certificate Issuer</th> <th>Valid Dates</th> </tr> </thead> <tbody> <tr> <td>*labs.oracle.com</td> <td>HTTPS Wildcard</td> <td>Common Name: *labs.oracle.com Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 4, 2015, 4:57 pm To: October 4, 2015, 4:57 pm</td> </tr> </tbody> </table> <p>Establish SSO Zone Create CSR Update Delete Report</p> <p>The PMAC web server restarts immediately to put the default certificate into effect. Users now have to acknowledge and accept the certificate when accessing the PMAC GUI. For this reason, the current session may need to be re-established.</p> | Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | *labs.oracle.com | HTTPS Wildcard | Common Name: *labs.oracle.com Organization: Oracle | Self-Signed | From: September 4, 2015, 4:57 pm To: October 4, 2015, 4:57 pm |
| Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | | | | | | | |
| *labs.oracle.com | HTTPS Wildcard | Common Name: *labs.oracle.com Organization: Oracle | Self-Signed | From: September 4, 2015, 4:57 pm To: October 4, 2015, 4:57 pm | | | | | | | |

9.28 Use the PMAC File Management System

This procedure uses the PMAC GUI to manage files on the PMAC server. These files are stored locally in the `/var/TKLC/db/filemgmt/csr` directory (considered the FMA or File Management Area). Any files added to the FMA are visible from the **Status and Management > Files** screen on the PMAC GUI. Up to 20 files are visible on the page. After that, scrollbars are enabled to view the remaining files.

Note: Do not manually copy files to the FMA. Currently only Certificate Signing Request (CSR) files are stored in the FMA when Certificates are created (see Certificate Management).

There are three possible actions, which can be invoked on a file:

- Delete - Select one or more files to be deleted.
- View - View a single selected file.
- Download - Download to the client browser a single selected file.

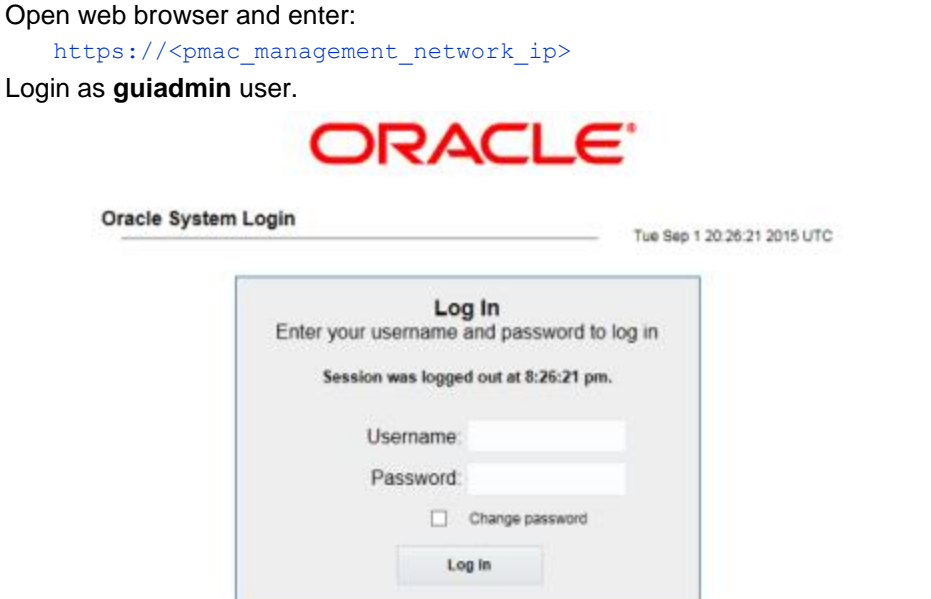
Prerequisite: You must be logged in as the Admin user to access this page.

9.28.1 Use the PMAC File Management System to Delete Files

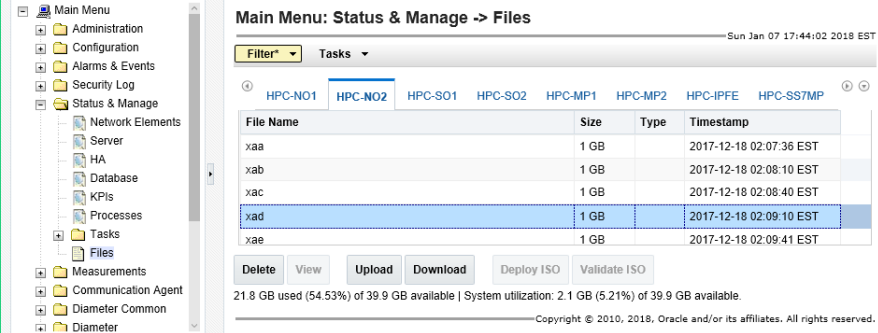
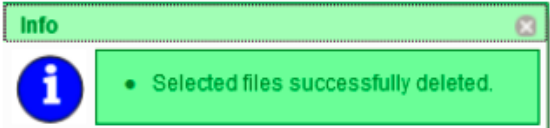
This procedure deletes one of more files on the PMAC server using the PMAC GUI.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 84. Use the PMAC File Management System to Delete Files

| Step | Procedure | Results |
|--------------------------------|---------------------------|---|
| 1. <input type="checkbox"/> | PMAC GUI: Login | Open web browser and enter: <code>https://<pmac_management_network_ip></code> Login as guiadmin user.  |

Procedure 84. Use the PMAC File Management System to Delete Files


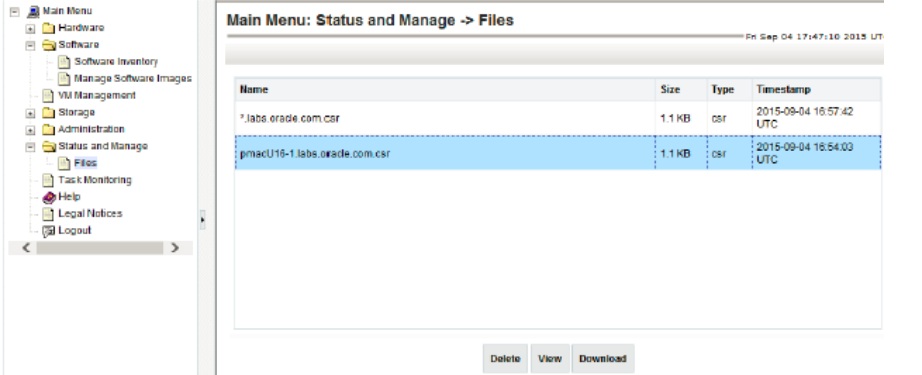
| Step | Procedure | Results |
|---|---------------------------|---|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>Select a file</p> | <ol style="list-style-type: none"> Navigate to Status and Management > Files. Select one or more files to delete.  <p>Upon initial display of the Files Management screen, all available files located within the FMA are visible.</p> <p>If no files are located within the FMA, There are no files present displays.</p> <p>If no files are selected, all buttons are visible but disabled. If a single file is selected all buttons are enabled. If more than one file is selected, the View and Download buttons are disabled.</p> |
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Delete the file(s)</p> | <ol style="list-style-type: none"> Click Delete. Click OK to confirm. <p>The Files Management screen refreshes with the selected file(s) no longer displayed and a status info box (which can be selected) indicating the action was successful.</p>  |

9.28.2 Use the PMAC File Management System to View Files

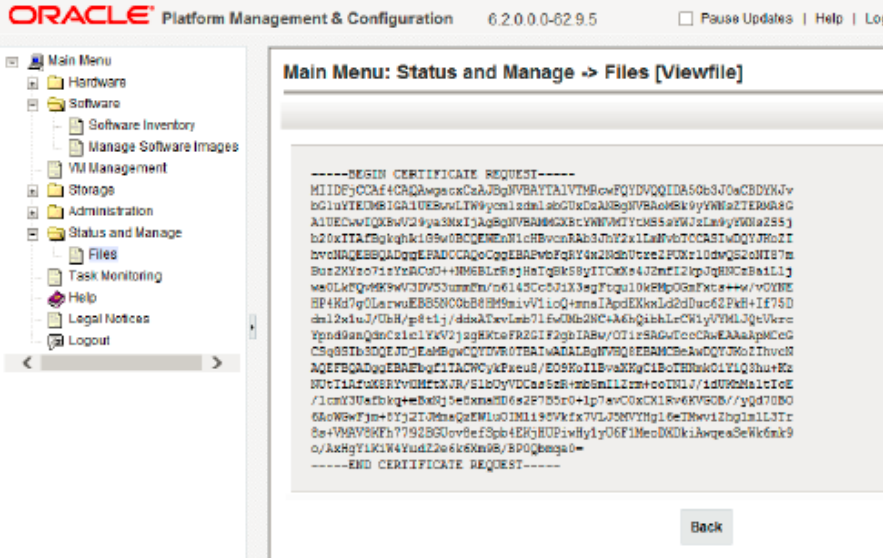
This procedure views a single file on the PMAC server using the PMAC GUI.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 85. Use the PMAC File Management System

| Step | Procedure | Results |
|------------------------------------|-----------------------------------|---|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guidadmin user.</p>  |
| <p>2. <input type="checkbox"/></p> | <p>Select a file</p> | <p>1. Navigate to Status and Management > Files. 2. Select one file to view.</p>  <p>Only one file may be selected for viewing. If more than one file is selected, the View and Download buttons are disabled.</p> |

Procedure 85. Use the PMAC File Management System


| Step | Procedure | Results |
|---|-------------------------|---|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>View single file</p> | <p>The View File page displays.</p>  <p>Click the Back arrow to return to the original Files Management screen.</p> |

9.28.3 Use the PMAC File Management System to Download Files

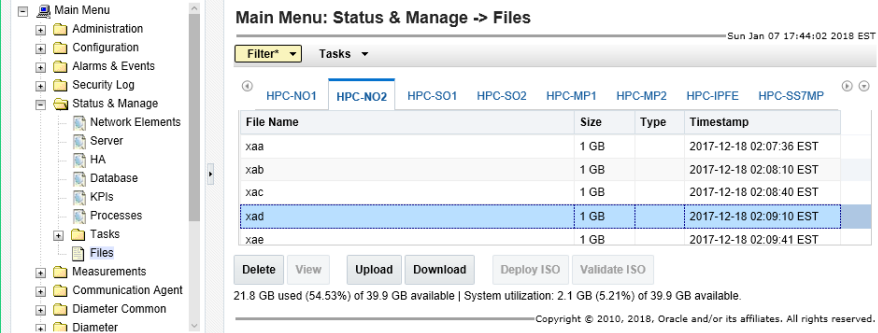
This procedure downloads a single file to the PMAC server using the PMAC GUI.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 86. Use the PMAC File Management System

| Step | Procedure | Results |
|---|-----------------------------------|---|
| <p>1.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guidadmin user.</p>  |

Procedure 86. Use the PMAC File Management System

| Step | Procedure | Results |
|---|-------------------------------|--|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>Select a file</p> | <p>1. Navigate to Status and Management > Files.</p> <p>2. Select one file to download.</p>  <p>Only one file may be selected for downloading. If more than one file is selected, the View and Download buttons are disabled.</p> |
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Download a single file</p> | <p>1. Click Delete.</p> <p>2. Depending on the browser, you are asked to Save to a disk or Open the file.</p> <p>The default editor program (usually set to Notepad, which does not format files) used by Internet Explorer can be changed (as of IE 9) by going to Tools > Internet Options > Programs > Set Programs > Associate a file type or protocol with a program and choosing the desired default editor for the given file type.</p> |

9.29 Delete ISO Images from the PMAC Image Repository


This procedure deletes ISO images from the PMAC repository.

Prerequisites:

9.8 Add ISO Images to the PMAC Image Repository

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 87. Delete ISO Images from the PMAC Image Repository

| Step | Procedure | Results | | | | | | | | | | | | | | | | |
|---|--|---|------------------------------|----------|--------------|-------------|------------------------------|---------|--------|--|---|----------|--------|--|------------------------------|----------|--------|--|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guidadmin user.</p>  | | | | | | | | | | | | | | | | |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select an image</p> | <p>1. Navigate to Software > Manage Software Images. 2. Select the software image to delete.</p> <p>Main Menu: Software -> Manage Software Images</p> <p>Fri Sep 04 19:11:27 2015 L</p> <p>Tasks ▾</p> <table border="1" data-bbox="550 1121 1365 1369"> <thead> <tr> <th>Image Name</th> <th>Type</th> <th>Architecture</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>PMAC-5.2.0.0.0_62.8.5-x86_64</td> <td>Upgrade</td> <td>x86_64</td> <td></td> </tr> <tr> <td>TPD.Install-7.0.2.0.0_85.28.0-OracleLinux6.6-x86_64</td> <td>Bootable</td> <td>x86_64</td> <td></td> </tr> <tr> <td>TVOE-3.2.0.0.0_88.8.0-x86_64</td> <td>Bootable</td> <td>x86_64</td> <td></td> </tr> </tbody> </table> <p>Add Image Edit Image Delete Selected</p> | Image Name | Type | Architecture | Description | PMAC-5.2.0.0.0_62.8.5-x86_64 | Upgrade | x86_64 | | TPD.Install-7.0.2.0.0_85.28.0-OracleLinux6.6-x86_64 | Bootable | x86_64 | | TVOE-3.2.0.0.0_88.8.0-x86_64 | Bootable | x86_64 | |
| Image Name | Type | Architecture | Description | | | | | | | | | | | | | | | |
| PMAC-5.2.0.0.0_62.8.5-x86_64 | Upgrade | x86_64 | | | | | | | | | | | | | | | | |
| TPD.Install-7.0.2.0.0_85.28.0-OracleLinux6.6-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | |
| TVOE-3.2.0.0.0_88.8.0-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | |
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Delete the image</p> | <p>1. Click Delete Image. 2. Click OK to confirm.</p> <p>The Manage Software Images screen refreshes with the selected file(s) no longer displayed. Click Info to confirm the correct image file was deleted.</p> <p>Main Menu: Software -> Manage Software Images</p> <p>Fri Sep</p> <p>Info ▾ Tasks ▾</p> <div data-bbox="516 1688 1252 1822"> <p>Info</p> <ul style="list-style-type: none"> • Software image PMAC-5.2.0.0.0_62.8.5-x86_64 has been deleted from OS distribution repository • Task ID: 102 </div> <table border="1" data-bbox="550 1801 1252 1822"> <tbody> <tr> <td>TVOE-3.2.0.0.0_88.8.0-x86_64</td> <td>Bootable</td> <td>x86_64</td> <td></td> </tr> </tbody> </table> | TVOE-3.2.0.0.0_88.8.0-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | |
| TVOE-3.2.0.0.0_88.8.0-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | |

9.30 Configure PMAC Domain Name System



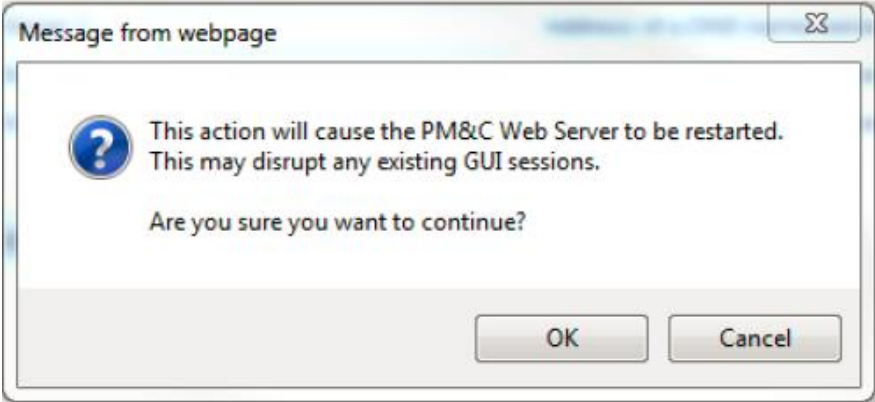
This procedure configures the PMAC Domain Name System (DNS).

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.



Procedure 88. Configure PMAC Domain Name System

| Step | Procedure | Results |
|------------------------------------|---|--|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Update the domain server only</p> | <ol style="list-style-type: none"> Navigate to Administration > Remote Servers > DNS Configuration. On initial setup, all fields should be empty. Enter the required Domain name. This should be a valid domain name consisting of 1 to 255 alphanumeric characters plus the "." and "-" characters. Leave all Name Server text boxes blank. Click Update DNS Configuration. <p>Main Menu: Administration -> Remote Servers -> DNS Configuration <small>Fri Sep 04 18:21:07 2015</small></p> <hr/> <p>System Domain Domain Name <input type="text" value="labs.oracle.com"/> <small>Note: The Domain Name value may only contain alphanumeric, hyphen, and decimal characters. Length must be 1 to 255 chars.</small></p> <p>External DNS Name Servers Name Server 1 Address <input type="text"/> Name Server 2 Address <input type="text"/> Name Server 3 Address <input type="text"/> <small>Note: Each Name Server Address value must be a IPv4 address, IPv6 address, or blank.</small></p> <hr/> <p>Update DNS Configuration</p> <p>This saves the Domain Name into the PMAC database. It does not enable DNS for the PMAC. After the update, the DNS Configuration refreshes with the domain name displayed in the Domain textbox.</p> <p>It does not update the DNS /etc/resolv.conf file. This file is in the following format (TPD default):</p> <pre># Generated by NetworkManager # No nameservers found; try putting DNS servers into your # ifcfg files in /etc/sysconfig/network-scripts like so: # # DNS1=xxx.xxx.xxx.xxx # DNS2=xxx.xxx.xxx.xxx # DOMAIN=lab.foo.com bar.foo.com \$ cat /etc/resolv.conf # Generated by NetworkManager</pre> <ol style="list-style-type: none"> Check for errors. <p>Success:</p> |

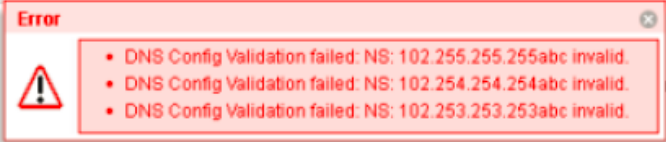
Procedure 88. Configure PMAC Domain Name System

| Step | Procedure | Results |
|------------------------------------|---|--|
| | |  <p>Error:</p>  <p>5. Click OK to confirm the web server restart.</p>  <p>6. Refresh the DNS Configuration screen since the web server restarted.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Update the full DNS configuration</p> | <ol style="list-style-type: none"> 1. Navigate to Administration > Remote Servers > DNS Configuration. 2. On initial setup, all fields should be empty. Enter the required Domain name. This should be a valid domain name consisting of 1 to 255 alphanumeric characters plus the "." and "-" characters. Leave all Name Server text boxes blank. 3. Type a valid IPv4 or IPv6 address in each Name Server textbox. It is not required to type an IP into all three textboxes. 4. Click Update DNS Configuration. |

Procedure 88. Configure PMAC Domain Name System

| Step | Procedure | Results |
|------|-----------|--|
| | | <p>Main Menu: Administration -> Remote Servers -> DNS Configuration Fri Sep 04 18:28:44 2015 UTC</p> <hr/> <p>System Domain Domain Name <input type="text" value="labs.oracle.com"/> <small>Note: The Domain Name value may only contain alphanumeric, hyphen, and decimal characters. Length must be 1 to 255 chars.</small></p> <p>External DNS Name Servers Name Server 1 Address <input type="text" value="10.20.100.101"/> Name Server 2 Address <input type="text" value="10.20.100.102"/> Name Server 3 Address <input type="text"/></p> <p><small>Note: Each Name Server Address value must be a IPv4 address, IPv6 address, or blank</small></p> <hr/> <p>Update DNS Configuration</p> <p>This saves the Domain Name into the PMAC database and enables DNS for the PMAC. After the update, the DNS Configuration refreshes with the domain name displayed in the Domain textbox and all servers display. It also updates the DNS /etc/resolv.conf file. This file is in the following format (TPD default):</p> <pre># PMAC DNS Configuration File # ----- # WARNING: Do not make manual changes to this file. This # file # is auto generated by the PMAC GUI Application at # Administration->Remote Servers->DNS Configuration. domain labs.tekelec.com nameserver 102.255.255.255 nameserver 102.255.255.254 nameserver 102.255.255.253</pre> <p>5. Check for errors.</p> <p>Success:</p>  <p>Errors:</p> <ul style="list-style-type: none"> • Domain Name validation failure  <ul style="list-style-type: none"> • Server Name validation failure. This error may display a failure for each incorrect Name Server. |

Procedure 88. Configure PMAC Domain Name System

| Step | Procedure | Results |
|------------------------------------|--|---|
| | |  |
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Remove the current DNS configuration</p> | <ol style="list-style-type: none"> 1. Navigate to Administration > Remote Servers > DNS Configuration. 2. Delete all entries from all Name Server textboxes. This assumes the Certificates Management screen is still using the Domain Name. 3. Click Update DNS Configuration. <p>Main Menu: Administration -> Remote Servers -> DNS Configuration</p> <p style="text-align: right;">Fri Sep 04 18:21:57 201</p> <hr/> <p>System Domain</p> <p>Domain Name <input type="text" value="labs.oracle.com"/></p> <p>Note: The Domain Name value may only contain alphanumeric, hyphen, and decimal characters. Length must be 1 to 255 chars.</p> <p>External DNS Name Servers</p> <p>Name Server 1 Address <input type="text"/></p> <p>Name Server 2 Address <input type="text"/></p> <p>Name Server 3 Address <input type="text"/></p> <p>Note: Each Name Server Address value must be a IPv4 address, IPv6 address, or blank.</p> <hr/> <p><input type="button" value="Update DNS Configuration"/></p> <p>This saves the Domain Name into the PMAC database and disables DNS for the PMAC. After the update, the DNS Configuration refreshes with the domain name displayed in the Domain textbox and all servers are blank. It also updates the DNS <code>/etc/resolv.conf</code> file. This file is in the following format (TPD default):</p> <pre># Generated by NetworkManager # No nameservers found; try putting DNS servers into your # ifcfg files in /etc/sysconfig/network-scripts like so: # # DNS1=xxx.xxx.xxx.xxx # DNS2=xxx.xxx.xxx.xxx # DOMAIN=lab.foo.com bar.foo.com \$ cat /etc/resolv.conf # Generated by NetworkManager</pre> |

9.31 Set User Authentication on the PMAC

This procedure configures the authentication on a new or existing user from the **Main Menu > Administration > Access Control > Users** screen by clicking **Insert** for new users or selecting an existing user entry and clicking **Edit**. Remote Authentication can only be used if an LDAP server has been properly configured on the PMAC. Please see section 9.33 Configure an LDAP Server on the PMAC for information regarding LDAP Server configuration.

When creating a new user or updating an existing user, the **Authentication Options - Allow Local Authentication** checkbox is initially marked. The user must apply the following rules when selecting the authentication type:

1. The three default users (guiadmin, pmacops, and guest) have a default setting of **Allow Local Authentication** selected and **Allow Remote Authentication** not selected. On upgrade, these settings are configured according to the setting of the **GUI Site Settings > Local Authentication Enabled** (if included in the **from** release).
2. The guiadmin user authentication settings cannot be changed and is disabled. All other user authentication settings are configurable.
3. The authentication settings for each user (except for the guiadmin user) can be **Allow Local Authentication** or **Allow Remote Authentication** only selected, both **Allow Local Authentication** and **Allow Remote Authentication** selected, or neither selected.
4. If a user is created with neither authentication selected, the user fails local authentication unless it is an admin group user. It does not attempt remote authentication.
5. If a new user is created with **Allow Remote Authentication** only selected, on first login, the password change request is not initiated. Once **Allow Local Authentication** is selected for the new user, the user is asked to change the password on the next login. After the password change, operation behaves normally.
6. If both **Allow Local Authentication** and **Allow Remote Authentication** are selected, the system attempts remote authentication first. If communication is established to the LDAP server for authentication and authentication fails, local authentication is not attempted. The login is rejected.
7. If both **Allow Local Authentication** and **Allow Remote Authentication** are selected, the system attempts remote authentication first. If communication is NOT established to the LDAP server for authentication, local authentication is attempted. The login request is accepted if the proper local credentials are used.
8. The local password and the remote password do not have to be the same. When logging in, the user must use the appropriate password for the given authentication method. For remote authentication, it is not necessary to enter the password since it is maintained on the LDAP server.

9.32 Configure the PMAC into an Existing Single Sign-On (SSO) Domain

This procedure set up and incorporates the PMAC into an existing single sign-on domain. Within a given domain (SSO can only configured with a sing domain), the PMAC is defined within a different domain zone the NO/SO/MP. The SSO certificates of the different zones must be imported manually using the Certificate Management interface of the two zones (typically from the AppWorks GUI and the PMAC GUI). Once each zone includes the local and remote SSO certificates, the user can login from one zone management GUI, which then logs the user into the other zone management GUIs

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 89. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

| Step | Results | | | | | | | | | | |
|--------------------------------|---|---|--------------------|--|--------------------|-------------|-------|-----------|---|-------------|--|
| 1. <input type="checkbox"/> | There must be a common user defined on both zones with the same group privileges. This user can be configured to use local or remote authentication (see 9.31 Set User Authentication on the PMAC). | | | | | | | | | | |
| 2. <input type="checkbox"/> | <p>The current zone (ZoneA - consisting of the NO/SO/MP architecture) should already have an existing SSO certificate configured from the Administration > Access Control > Certificate Management screen using the Establish SSO Zone button. This is indicated as the SSO Local certificate type.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management Tue Sep 08 19:10:19 2015 UTC</p> <table border="1"> <thead> <tr> <th>Certificate Name</th> <th>Certificate Type</th> <th>Certificate Subject</th> <th>Certificate Issuer</th> <th>Valid Dates</th> </tr> </thead> <tbody> <tr> <td>ZoneA</td> <td>SSO Local</td> <td>Common Name: ZoneA\domain=labs.oracle.com\type=AWS SO Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm</td> </tr> </tbody> </table> <p>Reestablish SSO Zone Create CSR Import Delete Report</p> | Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | ZoneA | SSO Local | Common Name: ZoneA\domain=labs.oracle.com\type=AWS SO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm |
| Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | | | | | | | |
| ZoneA | SSO Local | Common Name: ZoneA\domain=labs.oracle.com\type=AWS SO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm | | | | | | | |
| 3. <input type="checkbox"/> | <p>1. From the ZoneB (PMAC) GUI, navigate to Administration > Access Control > Certificate Management.</p> <p>2. Click Establish SSO Zone.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management [Establish SSO Zone] Tue Sep 08 19:05:23 2015 UTC</p> <p>Zone Name * <input type="text"/> Name of the SSO-compatible local zone. [Range = A 1-15 character long string. Allowed characters are A-Z, a-z,0-9]. [A value is required.]</p> <p>Ok Apply Cancel</p> | | | | | | | | | | |

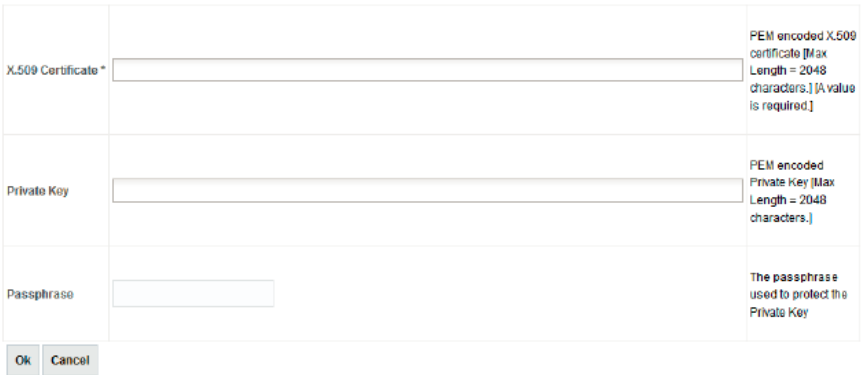
Procedure 89. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

| Step | Results | | | | | | | | | | |
|------------------------------------|---|--|----------------------|--|--------------------|----------------------|---|------------|--|--|--|
| <p>4. <input type="checkbox"/></p> | <p>1. Enter a valid Zone Name.</p> <p>2. Click OK.</p> <p>This creates a SSO Local certificate on the PMAC and returns to Administration > Access Control > Certificate Management.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management Tue Sep 08 19:08:31 2015 UTC</p> <table border="1"> <thead> <tr> <th>Certificate Name</th> <th>Certificate Type</th> <th>Certificate Subject</th> <th>Certificate Issuer</th> <th>Valid Dates</th> </tr> </thead> <tbody> <tr> <td>ZoneB</td> <td>SSO Local</td> <td>Common Name: ZoneB/domain=iabs.oracle.com/type=AWS SSO Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 8, 2015, 7:08 pm To: September 7, 2016, 7:08 pm</td> </tr> </tbody> </table> <p>Reestablish SSO Zone Create CSR Import Delete Report</p> | Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | ZoneB | SSO Local | Common Name: ZoneB/domain=iabs.oracle.com/type=AWS SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:08 pm To: September 7, 2016, 7:08 pm |
| Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | | | | | | | |
| ZoneB | SSO Local | Common Name: ZoneB/domain=iabs.oracle.com/type=AWS SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:08 pm To: September 7, 2016, 7:08 pm | | | | | | | |
| <p>5. <input type="checkbox"/></p> | <p>1. From ZoneA (AppWorks) GUI, navigate to Administration > Access Control > Certificate Management.</p> <p>2. Select the ZoneA SSO Local certificate and click Report.</p> <p>This displays a printable encrypted version of the certificate.</p> | | | | | | | | | | |
| <p>6. <input type="checkbox"/></p> | <p>Copy the certificate from the -----BEGIN CERTIFICATE----- to the end of the -----END CERTIFICATE-----.</p> | | | | | | | | | | |
| <p>7. <input type="checkbox"/></p> | <p>Click Back to return to Administration > Access Control > Certificate Management.</p> | | | | | | | | | | |
| <p>8. <input type="checkbox"/></p> | <p>Navigate to the ZoneB (PMAC) GUI Administration > Access Control > Certificate Management.</p> | | | | | | | | | | |
| <p>9. <input type="checkbox"/></p> | <p>Click Import.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management [Import Certificate] Fri Sep 04 17:06:09 2015 UTC</p> <table border="1"> <tbody> <tr> <td>X.509 Certificate *</td> <td><input type="text"/></td> <td>PEM encoded X.509 certificate [Max Length = 2048 characters.] [A value is required.]</td> </tr> <tr> <td>Private Key</td> <td><input type="text"/></td> <td>PEM encoded Private Key [Max Length = 2048 characters.]</td> </tr> <tr> <td>Passphrase</td> <td><input type="text"/></td> <td>The passphrase used to protect the Private Key</td> </tr> </tbody> </table> <p>Ok Cancel</p> | X.509 Certificate * | <input type="text"/> | PEM encoded X.509 certificate [Max Length = 2048 characters.] [A value is required.] | Private Key | <input type="text"/> | PEM encoded Private Key [Max Length = 2048 characters.] | Passphrase | <input type="text"/> | The passphrase used to protect the Private Key | |
| X.509 Certificate * | <input type="text"/> | PEM encoded X.509 certificate [Max Length = 2048 characters.] [A value is required.] | | | | | | | | | |
| Private Key | <input type="text"/> | PEM encoded Private Key [Max Length = 2048 characters.] | | | | | | | | | |
| Passphrase | <input type="text"/> | The passphrase used to protect the Private Key | | | | | | | | | |

Procedure 89. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

| Step | Results | | | | | | | | | | | | | | | |
|---------------------------------|--|---|--------------------|--|--------------------|-------------|-------|-----------|---|-------------|--|-------|------------|---|-------------|--|
| 10. <input type="checkbox"/> | Paste the copied certificate from ZoneA into the X.509 Certificate field. Leave the other fields blank. | | | | | | | | | | | | | | | |
| 11. <input type="checkbox"/> | <p>Click OK.</p> <p>This creates a Remote SSO certificate and returns to Administration > Access Control > Certificate Management displaying ZoneB as the SSO Local certificate type and ZoneA as the SSO Remote certificate type.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management</p> <p style="text-align: right;">Tue Sep 08 19:15:20 2015 UTC</p> <table border="1" data-bbox="300 625 1156 823"> <thead> <tr> <th>Certificate Name</th> <th>Certificate Type</th> <th>Certificate Subject</th> <th>Certificate Issuer</th> <th>Valid Dates</th> </tr> </thead> <tbody> <tr> <td>ZoneB</td> <td>SSO Local</td> <td>Common Name: ZoneB/domain=labs.oracle.com/type=AW SSO Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 8, 2015, 7:14 pm To: September 7, 2016, 7:14 pm</td> </tr> <tr> <td>ZoneA</td> <td>SSO Remote</td> <td>Common Name: ZoneA/domain=labs.oracle.com/type=AW SSO Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm</td> </tr> </tbody> </table> <p style="text-align: center;">< ></p> <p> <input type="button" value="Reestablish SSO Zone"/> <input type="button" value="Create CSR"/> <input type="button" value="Import"/> <input type="button" value="Delete"/> <input type="button" value="Report"/> </p> | Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | ZoneB | SSO Local | Common Name: ZoneB/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:14 pm To: September 7, 2016, 7:14 pm | ZoneA | SSO Remote | Common Name: ZoneA/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm |
| Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | | | | | | | | | | | | |
| ZoneB | SSO Local | Common Name: ZoneB/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:14 pm To: September 7, 2016, 7:14 pm | | | | | | | | | | | | |
| ZoneA | SSO Remote | Common Name: ZoneA/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm | | | | | | | | | | | | |
| 12. <input type="checkbox"/> | <p>3. From ZoneB (PMAC) GUI, navigate to Administration > Access Control > Certificate Management.</p> <p>4. Select the ZoneB SSO Local certificate and click Report.</p> <p>This displays a printable encrypted version of the certificate.</p> | | | | | | | | | | | | | | | |
| 13. <input type="checkbox"/> | Copy the certificate from the -----BEGIN CERTIFICATE----- to the end of the -----END CERTIFICATE-----. | | | | | | | | | | | | | | | |
| 14. <input type="checkbox"/> | Click Back to return to Administration > Access Control > Certificate Management . | | | | | | | | | | | | | | | |
| 15. <input type="checkbox"/> | Navigate to the ZoneA (AppWorks) GUI Administration > Access Control > Certificate Management . | | | | | | | | | | | | | | | |

Procedure 89. Configure the PMAC into an Existing Single Sign-On (SSO) Domain

| Step | Results | | | | | | | | | | | | | | | |
|-------------------------------------|--|---|--------------------|--|--------------------|-------------|-------|------------|---|-------------|--|-------|-----------|---|-------------|--|
| <p>16.</p> <input type="checkbox"/> | <p>Click Import.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management [Import Certificate]</p> <p style="text-align: right;">Fri Sep 04 17:05:09 2015 UTC</p>  | | | | | | | | | | | | | | | |
| <p>17.</p> <input type="checkbox"/> | <p>Paste the copied certificate from ZoneB into the X.509 Certificate field. Leave the other fields blank.</p> | | | | | | | | | | | | | | | |
| <p>18.</p> <input type="checkbox"/> | <p>Click OK.</p> <p>This creates a Remote SSO certificate and returns to Administration > Access Control > Certificate Management displaying ZoneA as the SSO Local certificate type and ZoneB as the SSO Remote certificate type.</p> <p>Main Menu: Administration -> Access Control -> Certificate Management</p> <p style="text-align: right;">Tue Sep 08 19:15:20 2015 UTC</p> <table border="1" data-bbox="300 1150 1156 1348"> <thead> <tr> <th>Certificate Name</th> <th>Certificate Type</th> <th>Certificate Subject</th> <th>Certificate Issuer</th> <th>Valid Dates</th> </tr> </thead> <tbody> <tr> <td>ZoneB</td> <td>SSO Remote</td> <td>Common Name: ZoneB/domain=labs.oracle.com/type=AW SSO Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 8, 2015, 7:14 pm To: September 7, 2016, 7:14 pm</td> </tr> <tr> <td>ZoneA</td> <td>SSO Local</td> <td>Common Name: ZoneA/domain=labs.oracle.com/type=AW SSO Organization: Oracle</td> <td>Self-Signed</td> <td>From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm</td> </tr> </tbody> </table> <p style="text-align: center;">< ></p> <p>Reestablish SSO Zone Create CSR Import Delete Report</p> <p>Once both zones have their local and remote SSO certificates configured, the user is able to login from ZoneA or ZoneB using the configured user that is defined on both zones. Once logged in from one zone, the other zone GUI logs in immediately.</p> <p>If the user logs out from either zone, both zones are logged out.</p> <p>If a user logs in from ZoneA, which logs in ZoneB, and later the ZoneB session times out due to a short session timeout settings configured on ZoneB, ZoneA remains logged in. This works the same in either direction.</p> | Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | ZoneB | SSO Remote | Common Name: ZoneB/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:14 pm To: September 7, 2016, 7:14 pm | ZoneA | SSO Local | Common Name: ZoneA/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm |
| Certificate Name | Certificate Type | Certificate Subject | Certificate Issuer | Valid Dates | | | | | | | | | | | | |
| ZoneB | SSO Remote | Common Name: ZoneB/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:14 pm To: September 7, 2016, 7:14 pm | | | | | | | | | | | | |
| ZoneA | SSO Local | Common Name: ZoneA/domain=labs.oracle.com/type=AW SSO Organization: Oracle | Self-Signed | From: September 8, 2015, 7:10 pm To: September 7, 2016, 7:10 pm | | | | | | | | | | | | |

9.33 Configure an LDAP Server on the PMAC

This procedure configures a LDAP server on the PMAC.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 90. Configure an LDAP Server on the PMAC

| Step | Results | | | | | | | | | | | | | | | | | | | | | |
|---|---|--|----------------------|--|---------------------|----------------------|---|---------------------------|----------------------|--|------------------|----------------------------------|---|-----------|----------------------|---|----------|----------------------|---|--|----------------------|--|
| <p>1.</p> <p><input type="checkbox"/></p> | <p>Navigate to Administration > Remote Servers > LDAP Authentication.</p> <p>Main Menu: Administration -> Remote Servers -> LDAP Authentication</p> <p style="text-align: right;">Tue Sep 08 19:31:23 2015 UTC</p> <table border="1" data-bbox="305 619 1161 682"> <thead> <tr> <th>Hostname</th> <th>Domain Name</th> <th>Domain Name Short</th> <th>Port</th> <th>Canonic Form</th> <th>Base DN</th> <th>Username</th> <th>Filter Format</th> <th>Follow Referral</th> <th>Bind Requires DN</th> </tr> </thead> <tbody> <tr> <td colspan="10" style="text-align: center;">(Empty table)</td> </tr> </tbody> </table> <p><input type="button" value="Insert"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Report"/> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Test Server"/></p> <p>Only Insert and Report are available and no LDAP servers configured.</p> | Hostname | Domain Name | Domain Name Short | Port | Canonic Form | Base DN | Username | Filter Format | Follow Referral | Bind Requires DN | (Empty table) | | | | | | | | | | |
| Hostname | Domain Name | Domain Name Short | Port | Canonic Form | Base DN | Username | Filter Format | Follow Referral | Bind Requires DN | | | | | | | | | | | | | |
| (Empty table) | | | | | | | | | | | | | | | | | | | | | | |
| <p>2.</p> <p><input type="checkbox"/></p> | <p>1. Click Insert.</p> <p>Main Menu: Administration -> Remote Servers -> LDAP Authentication [Insert]</p> <p style="text-align: right;">Tue Sep 08 19:40:10 2015 UTC</p> <p>Adding new LDAP account</p> <table border="1" data-bbox="300 1060 1161 1627"> <tbody> <tr> <td>Hostname *</td> <td><input type="text"/></td> <td>Unique name for the server. It can be either a valid IPv4 or IPv6 address or a valid hostname. Hostname must be unique and case-insensitive. The length should not exceed 255 characters. Valid hostname characters include alphanumeric characters (a-z), (A-Z), (0-9), period (.), or minus sign (-). The first character of a hostname must be an alpha character. [Range = A 1-255 character string.] [A value is required.]</td> </tr> <tr> <td>Account Domain Name</td> <td><input type="text"/></td> <td>Domain name of the LDAP server. Use following form: <name>.<did> (ex. oracle.com). [Range = A 1-29 character string. Allowed characters are A-Z, a-z, 0-9 and periods.]</td> </tr> <tr> <td>Account Domain Name Short</td> <td><input type="text"/></td> <td>The NetBIOS domain of the server. This is the shorter version of the account domain name listed above (ex. ORACLE). Must be a capitalized version of the domain name, without the extension. [Range = A 1-10 character string. Allowed characters are A-Z, 0-9.]</td> </tr> <tr> <td>Port *</td> <td><input type="text" value="389"/></td> <td>Port that the LDAP servers can be accessed by on the host machine [Default = 389. Range = Integer with value between 0 and 65535.] [A value is required.]</td> </tr> <tr> <td>Base DN *</td> <td><input type="text"/></td> <td>Directory path of the user being authenticated. [Range = A 1-100 long character string.] [A value is required.]</td> </tr> <tr> <td>Username</td> <td><input type="text"/></td> <td>User DN used for account DN lookups (not the user being authenticated.)</td> </tr> <tr> <td></td> <td><input type="text"/></td> <td>The password of the user DN used for account lookups. Password restrictions.</td> </tr> </tbody> </table> <p>Note: Port 389 has been set as default. This is the standard port number for LDAP communication. Change it, if necessary.</p> <p>2. Contact your LDAP Server Administrator for the proper values required to configure the LDAP server.</p> | Hostname * | <input type="text"/> | Unique name for the server. It can be either a valid IPv4 or IPv6 address or a valid hostname. Hostname must be unique and case-insensitive. The length should not exceed 255 characters. Valid hostname characters include alphanumeric characters (a-z), (A-Z), (0-9), period (.), or minus sign (-). The first character of a hostname must be an alpha character. [Range = A 1-255 character string.] [A value is required.] | Account Domain Name | <input type="text"/> | Domain name of the LDAP server. Use following form: <name>.<did> (ex. oracle.com). [Range = A 1-29 character string. Allowed characters are A-Z, a-z, 0-9 and periods.] | Account Domain Name Short | <input type="text"/> | The NetBIOS domain of the server. This is the shorter version of the account domain name listed above (ex. ORACLE). Must be a capitalized version of the domain name, without the extension. [Range = A 1-10 character string. Allowed characters are A-Z, 0-9.] | Port * | <input type="text" value="389"/> | Port that the LDAP servers can be accessed by on the host machine [Default = 389. Range = Integer with value between 0 and 65535.] [A value is required.] | Base DN * | <input type="text"/> | Directory path of the user being authenticated. [Range = A 1-100 long character string.] [A value is required.] | Username | <input type="text"/> | User DN used for account DN lookups (not the user being authenticated.) | | <input type="text"/> | The password of the user DN used for account lookups. Password restrictions. |
| Hostname * | <input type="text"/> | Unique name for the server. It can be either a valid IPv4 or IPv6 address or a valid hostname. Hostname must be unique and case-insensitive. The length should not exceed 255 characters. Valid hostname characters include alphanumeric characters (a-z), (A-Z), (0-9), period (.), or minus sign (-). The first character of a hostname must be an alpha character. [Range = A 1-255 character string.] [A value is required.] | | | | | | | | | | | | | | | | | | | | |
| Account Domain Name | <input type="text"/> | Domain name of the LDAP server. Use following form: <name>.<did> (ex. oracle.com). [Range = A 1-29 character string. Allowed characters are A-Z, a-z, 0-9 and periods.] | | | | | | | | | | | | | | | | | | | | |
| Account Domain Name Short | <input type="text"/> | The NetBIOS domain of the server. This is the shorter version of the account domain name listed above (ex. ORACLE). Must be a capitalized version of the domain name, without the extension. [Range = A 1-10 character string. Allowed characters are A-Z, 0-9.] | | | | | | | | | | | | | | | | | | | | |
| Port * | <input type="text" value="389"/> | Port that the LDAP servers can be accessed by on the host machine [Default = 389. Range = Integer with value between 0 and 65535.] [A value is required.] | | | | | | | | | | | | | | | | | | | | |
| Base DN * | <input type="text"/> | Directory path of the user being authenticated. [Range = A 1-100 long character string.] [A value is required.] | | | | | | | | | | | | | | | | | | | | |
| Username | <input type="text"/> | User DN used for account DN lookups (not the user being authenticated.) | | | | | | | | | | | | | | | | | | | | |
| | <input type="text"/> | The password of the user DN used for account lookups. Password restrictions. | | | | | | | | | | | | | | | | | | | | |

Procedure 90. Configure an LDAP Server on the PMAC

| Step | Results | | | | | | | | | | | | | | | | | | | | |
|----------------------|---|-------------------|-------------|-------------------|---------|--------------|---------------|-----------------|------------------|-----------------|------------------|----------------------|-----------------|--------|-----|-----------|--------|--|--|--------|----------|
| <p>3.</p> | <p>1. Click OK.</p> <p>The LDAP server configures and returns to Administration > Remote Servers > LDAP Authentication.</p> <p>Note: Click Apply to remain on the Insert screen.</p> <p>Main Menu: Administration -> Remote Servers -> LDAP Authentication</p> <p style="text-align: right;">Tue Sep 08 19:46:35 2015 UTC</p> <div data-bbox="300 506 1166 793"> <table border="1"> <thead> <tr> <th>Hostname</th> <th>Domain Name</th> <th>Domain Name Short</th> <th>Port</th> <th>Canonic Form</th> <th>Base DN</th> <th>Username</th> <th>Filter Format</th> <th>Follow Referral</th> <th>Bind Requires DN</th> </tr> </thead> <tbody> <tr> <td>ldap.labs.oracle.com</td> <td>labs.oracle.com</td> <td>ORACLE</td> <td>389</td> <td>Backslash</td> <td>dc=com</td> <td></td> <td></td> <td>IGNORE</td> <td>Disabled</td> </tr> </tbody> </table> <p>Buttons: Insert, Edit, Delete, Report, Move Up, Move Down, Test Server</p> </div> <p>2. Click Test Server.</p> <div data-bbox="292 856 862 1100"> <p>Test Server</p> <p>Username: <input type="text" value="username"/></p> <p>Password: <input type="password" value="*****"/></p> <p>Buttons: OK, Cancel</p> </div> <p>Type a valid username and password configured on the LDAP server to verify the user and communication to the LDAP server.</p> <p>3. Click Report to display the configuration data of the LDAP.</p> <p>Main Menu: Administration -> Remote Servers -> LDAP Authentication [Report]</p> <p style="text-align: right;">Tue Sep 08 19:48:03 2015 UTC</p> <div data-bbox="342 1297 1214 1591"> <pre> Main Menu: Administration -> Remote Servers -> LDAP Authentication [Report] Tue Sep 08 19:48:03 2015 UTC Server_ID: 1 host: ldap.labs.oracle.com port: 389 useStartTls: False bindRequiresDn: False baseDn: dc=com accountCanonicalForm: Backslash accountDomainName: labs.oracle.com accountDomainNameShort: ORACLE optReferrals: IGNORE </pre> <p>Buttons: Print, Save, Back</p> </div> | Hostname | Domain Name | Domain Name Short | Port | Canonic Form | Base DN | Username | Filter Format | Follow Referral | Bind Requires DN | ldap.labs.oracle.com | labs.oracle.com | ORACLE | 389 | Backslash | dc=com | | | IGNORE | Disabled |
| Hostname | Domain Name | Domain Name Short | Port | Canonic Form | Base DN | Username | Filter Format | Follow Referral | Bind Requires DN | | | | | | | | | | | | |
| ldap.labs.oracle.com | labs.oracle.com | ORACLE | 389 | Backslash | dc=com | | | IGNORE | Disabled | | | | | | | | | | | | |

9.34 Transfer Image from PMAC Repository to Other Servers

This procedure transfers a software image from the PMAC image repository to servers managed by PMAC.


Prerequisites:

- Enclosures containing the blade servers or servers containing a TVOE host targeted for application install/upgrade have been configured using the 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- Rack mount servers targeted for application install/upgrade have been configured using 9.15 Add Rack Mount Server to the PMAC System Inventory.
- An image was added to the PMAC image repository using 9.8 Add ISO Images to the PMAC Image Repository.

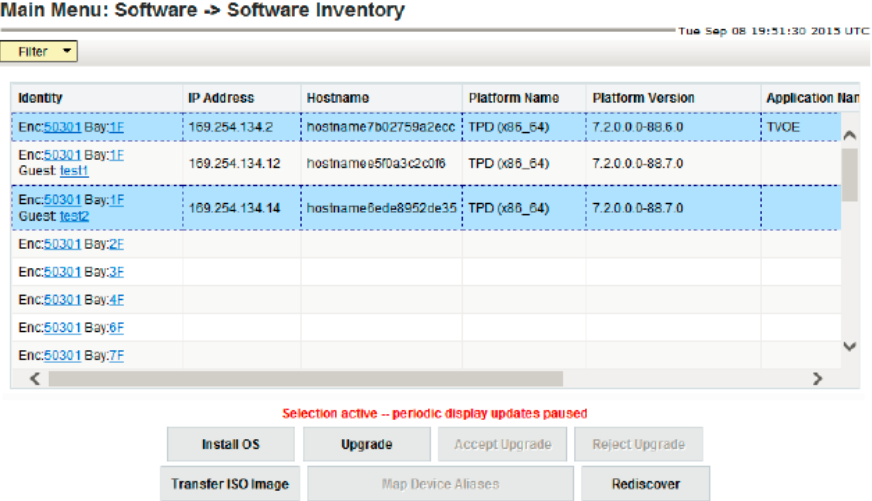
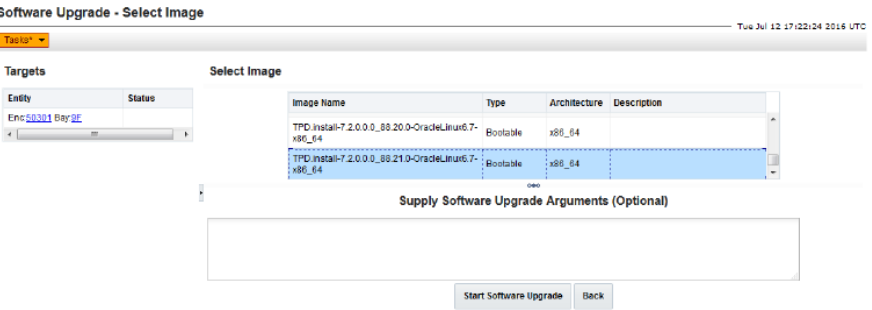
Note: The image transfer is only supported for discovered entities (IP address is known)

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 91. Transfer Image from PMAC Repository to Other Servers

| Step | Procedure | Results |
|--|-----------------------------------|--|
| <p>1. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>Open web browser and enter: <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as guiadmin user.</p>  <p>Navigate to Software > Software Inventory.</p> |

Procedure 91. Transfer Image from PMAC Repository to Other Servers

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|--|---------------|------------------|------------------|---------------|------------------|------------------|------------------|---------------|---|--------------|------------------|------|---|----------------|----------------------|--------------|------------------|--|-------------------------------|----------------|----------------------|--------------|------------------|--|------------------|--|--|--|--|--|------------------|--|--|--|--|--|------------------|--|--|--|--|--|------------------|--|--|--|--|--|------------------|--|--|--|--|--|
| <p>2. <input type="checkbox"/></p> | <p>PMAC GUI: Select servers</p> | <p>1. Select the servers where you want to transfer the image. If you want to perform an upgrade on more than one server, press Ctrl while selecting multiple rows.</p> <p>2. Click Transfer ISO Image.</p>  <p>Main Menu: Software -> Software Inventory</p> <p>Filter</p> <table border="1"> <thead> <tr> <th>Identity</th> <th>IP Address</th> <th>Hostname</th> <th>Platform Name</th> <th>Platform Version</th> <th>Application Name</th> </tr> </thead> <tbody> <tr> <td>Enc:50301 Bay:1E</td> <td>169.254.134.2</td> <td>hostname7b02759a2ecc</td> <td>TPD (x86_64)</td> <td>7.2.0.0.0-88.6.0</td> <td>TVOE</td> </tr> <tr> <td>Enc:50301 Bay:1E Guest: test1</td> <td>169.254.134.12</td> <td>hostnamee5f0a3c2c0f6</td> <td>TPD (x86_64)</td> <td>7.2.0.0.0-88.7.0</td> <td></td> </tr> <tr> <td>Enc:50301 Bay:1E Guest: test2</td> <td>169.254.134.14</td> <td>hostname0ede8952de35</td> <td>TPD (x86_64)</td> <td>7.2.0.0.0-88.7.0</td> <td></td> </tr> <tr> <td>Enc:50301 Bay:2E</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc:50301 Bay:3E</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc:50301 Bay:4E</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc:50301 Bay:6E</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Enc:50301 Bay:7E</td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p>Selection active -- periodic display updates paused</p> <p>Install OS Upgrade Accept Upgrade Reject Upgrade</p> <p>Transfer ISO Image Map Device Aliases Rediscover</p> | Identity | IP Address | Hostname | Platform Name | Platform Version | Application Name | Enc:50301 Bay:1E | 169.254.134.2 | hostname7b02759a2ecc | TPD (x86_64) | 7.2.0.0.0-88.6.0 | TVOE | Enc:50301 Bay:1E Guest: test1 | 169.254.134.12 | hostnamee5f0a3c2c0f6 | TPD (x86_64) | 7.2.0.0.0-88.7.0 | | Enc:50301 Bay:1E Guest: test2 | 169.254.134.14 | hostname0ede8952de35 | TPD (x86_64) | 7.2.0.0.0-88.7.0 | | Enc:50301 Bay:2E | | | | | | Enc:50301 Bay:3E | | | | | | Enc:50301 Bay:4E | | | | | | Enc:50301 Bay:6E | | | | | | Enc:50301 Bay:7E | | | | | |
| Identity | IP Address | Hostname | Platform Name | Platform Version | Application Name | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:1E | 169.254.134.2 | hostname7b02759a2ecc | TPD (x86_64) | 7.2.0.0.0-88.6.0 | TVOE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:1E Guest: test1 | 169.254.134.12 | hostnamee5f0a3c2c0f6 | TPD (x86_64) | 7.2.0.0.0-88.7.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:1E Guest: test2 | 169.254.134.14 | hostname0ede8952de35 | TPD (x86_64) | 7.2.0.0.0-88.7.0 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:3E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:4E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:6E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:7E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>3. <input type="checkbox"/></p> | <p>PMAC GUI: Select image</p> | <p>1. Select the image to transfer to the servers.</p> <p>2. Type the Path, User, and Password for the target entities.</p> <p>The credentials should be consistent with credentials used for SCP. The path should be accessible with the credentials provided.</p> <p>Note: PMAC does not validate firmware update arguments. It only verifies they are all present.</p> <p>3. Click Start Image Transfer.</p>  <p>Software Upgrade - Select Image</p> <p>Targets</p> <table border="1"> <thead> <tr> <th>Entity</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>Enc:50301 Bay:2E</td> <td></td> </tr> </tbody> </table> <p>Select Image</p> <table border="1"> <thead> <tr> <th>Image Name</th> <th>Type</th> <th>Architecture</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>TPD-Install-7.2.0.0_0_88.20.0-OracleLinux6.7-x86_64</td> <td>Bootable</td> <td>x86_64</td> <td></td> </tr> <tr> <td>TPD-Install-7.2.0.0_0_88.21.0-OracleLinux6.7-x86_64</td> <td>Bootable</td> <td>x86_64</td> <td></td> </tr> </tbody> </table> <p>Supply Software Upgrade Arguments (Optional)</p> <p>Start Software Upgrade Back</p> <p>4. Click OK to confirm the transfer.</p> | Entity | Status | Enc:50301 Bay:2E | | Image Name | Type | Architecture | Description | TPD-Install-7.2.0.0_0_88.20.0-OracleLinux6.7-x86_64 | Bootable | x86_64 | | TPD-Install-7.2.0.0_0_88.21.0-OracleLinux6.7-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Entity | Status | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enc:50301 Bay:2E | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Image Name | Type | Architecture | Description | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TPD-Install-7.2.0.0_0_88.20.0-OracleLinux6.7-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| TPD-Install-7.2.0.0_0_88.21.0-OracleLinux6.7-x86_64 | Bootable | x86_64 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 91. Transfer Image from PMAC Repository to Other Servers

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|--------------------------------------|---|-------------------------|-------------|-------------|--------|-------|-------------|----|---------------|----------------------------------|-------------------------|-------------|-----|----|---------------|------------------|-------------------------|-------------|-----|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|
| 4. <input type="checkbox"/> | PMAC GUI: Monitor transfer | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the Transfer background task. A separate task displays for each server.</p> <p>Main Menu: Task Monitoring Tue Sep 08 19:59:28 2015 UTC</p> <p>Filter <input type="text"/></p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Task Output</th> </tr> </thead> <tbody> <tr> <td>83</td> <td>File Transfer</td> <td>Enc:50301 Bay:1E Guest: test2</td> <td>File Transfer initiated</td> <td>IN_PROGRESS</td> <td>N/A</td> </tr> <tr> <td>82</td> <td>File Transfer</td> <td>Enc:50301 Bay:1E</td> <td>File Transfer initiated</td> <td>IN_PROGRESS</td> <td>N/A</td> </tr> <tr> <td>81</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>80</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>79</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>78</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>77</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>76</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Delete Completed"/> <input type="button" value="Delete Failed"/> <input type="button" value="Delete Selected"/> </p> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> | ID | Task | Target | Status | State | Task Output | 83 | File Transfer | Enc:50301 Bay:1E Guest: test2 | File Transfer initiated | IN_PROGRESS | N/A | 82 | File Transfer | Enc:50301 Bay:1E | File Transfer initiated | IN_PROGRESS | N/A | 81 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 80 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 79 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 78 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 77 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 76 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A |
| ID | Task | Target | Status | State | Task Output | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 83 | File Transfer | Enc:50301 Bay:1E Guest: test2 | File Transfer initiated | IN_PROGRESS | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 82 | File Transfer | Enc:50301 Bay:1E | File Transfer initiated | IN_PROGRESS | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 81 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 78 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 77 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 76 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

10. Configure SAN Procedures

10.1 Configure SAN Storage Using PMAC Application

This procedure configures a SAN storage using the PMAC application. You configure the SAN controller and corresponding host volumes using XML files uploaded by the PMAC application. The XML files allow you to:

- add virtual disks
- delete virtual disks without an associated volume
- add global spares
- delete global spares
- delete volumes on the SAN controller and/or host volume.

Refer to the instructions provided by the application to obtain or create XML files used in this procedure.

Prerequisites:

- 7.2 Configure Initial OA Settings Using the Configuration Wizard
- 9.5 Configure PMAC Application
- 5.3 Configure Advanced Settings on MSA 2012fc Fibre Channel Disk Controllers
- 5.4 Configure Advanced Settings on P2000 Fibre Channel Disk Controllers for a given SAN storage type
- 4.1 Configure Brocade Switches

Note: When a disk fails, the system looks for a dedicated spare first. If it does not find a properly sized dedicated spare, it looks for a global spare. A best practice is to designate spares for use if disks

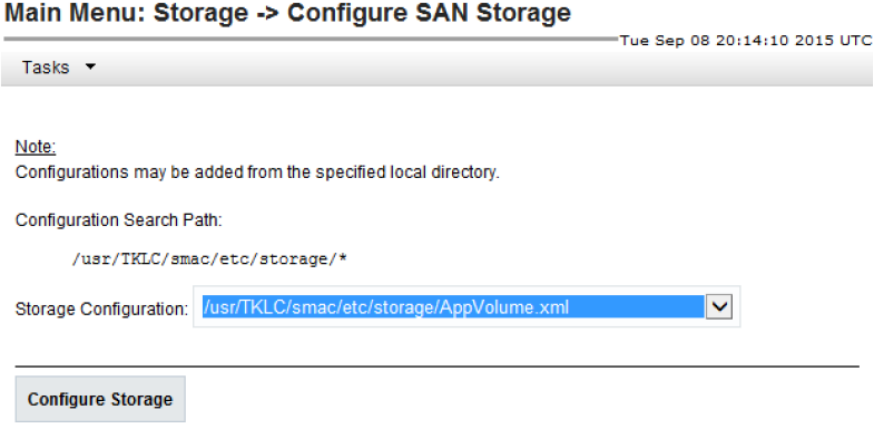
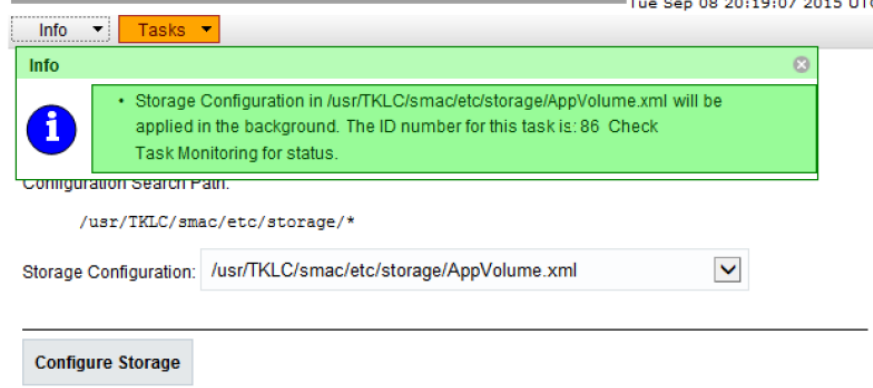
fail. Dedicating spares to vdisks is the most secure method, but it is also expensive to reserve spares for each vdisk. Alternatively, you can assign global spares. A properly sized spare is one whose capacity is equal to or greater than the largest disk in the vdisk.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 92. Configure SAN Storage Using PMAC Application

| Step | Procedure | Results |
|--|---|--|
| <p>1. <input type="checkbox"/></p> | <p>Handle failed SAN configuration</p> | <p>If any attempt to add SAN storage components have failed, a partial configuration may exist. This needs to be cleaned-up before attempting again. If an attempt to add SAN storage components fails before any configuration is done, such as an invalid XML file or a wrong disk name, then correct the XML file error and attempt the SAN storage configuration again.</p> <p>If a partial configuration exists, follow the instructions provided by application to obtain/create XML files that delete the partial configuration and clear the SAN controller or host volume. Note that after a host volume is deleted or cleared, PMAC automatically reboots the server blade. Once the XML file is obtained, continue following to correctly upload and execute the XML file using the PMAC application. If the end user desires to IPM the blade server to cleanup host volumes, refer to 9.9 IPM Servers Using PMAC Application.</p> |
| <p>2. <input type="checkbox"/></p> | <p>PMAC Server: Provide SAN configuration XML files</p> | <p>Log into the management server as the admusr user. Copy all SAN configuration XML files into /usr/TKLC/smac/etc/storage directory.</p> |
| <p>3. <input type="checkbox"/></p> | <p>PMAC Server: Update SAN controller password in PMAC</p> | <p>If default password has been changed on SAN controllers, then the stored password in PMAC must be changed to match. Run this script on PMAC and set the SAN controller password for the manage user:</p> <pre>\$ sudo /usr/TKLC/smac/bin/updateCredentials --type=msa</pre> |
| <p>4. <input type="checkbox"/></p> | <p>PMAC GUI: Login</p> | <p>If needed, open a web browser and type <a href="https://<pmac_management_network_ip>">https://<pmac_management_network_ip> Login as the guiadmin user.</p> |

Procedure 92. Configure SAN Storage Using PMAC Application

| Step | Procedure | Results |
|--|--|--|
| <p>5. <input type="checkbox"/></p> | <p>PMAC GUI: Configure SAN</p> | <p>Navigate to Main Men > Storage > Configure SAN Storage.</p> <p>From the Storage Configuration option, select SAN configuration file and click Configure Storage.</p> <p>Main Menu: Storage -> Configure SAN Storage</p>  <p>Note: Concurrent execution of SAN configuration files is supported. Do not run configuration files at the same time if the xml files configure either the same blade server or the same MSA storage system, otherwise a failure may occur . Additionally, configuration on a server blade is being cleared, or if a host volume is being deleted, then execution may take longer since PMAC automatically reboots the server blade after configuration removal.</p> <p>If any errors occur with this procedure, collect logs from the affected blade in /var/TKLC/log/tpdProvd/tpdProvd.log.</p> |
| <p>6. <input type="checkbox"/></p> | <p>PMAC GUI: Monitor configuration status</p> | <p>The Configure SAN Storage screen displays with a new background task entry. Click Tasks located on the toolbar.</p> <p>Main Menu: Storage -> Configure SAN Storage [Apply]</p>  |
| <p>7. <input type="checkbox"/></p> | <p>Recovery from configuration errors</p> | <p>If PMAC is able to parse the XML configuration file successfully, the configuration process is executed. If any error is encountered, the processing is aborted and the state is left as it was at the point of failure. For recovery suggestions, refer to step 1.</p> |

10.2 Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation

This procedure removes volumes from the partially installed SAN. This can happen if the SAN configuration fails. Blade servers are IPMed again.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 93. Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation

| Step | Procedure | Results |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Management Server: Update SAN controller password | If default password has been changed on SAN controllers, then the stored password in PMAC must be changed to match. Run this script on PMAC and set the SAN controller password for the manage user: <pre>\$ sudo /usr/TKLC/smac/bin/updateCredentials --type=msa</pre> |
| 2. <input type="checkbox"/> | Fibre Channel Controller GUI: Login | Log into <a href="https://<controller_IP_address>">https://<controller_IP_address> . |
| 3. <input type="checkbox"/> | Fibre Channel Controller GUI: Delete volumes and vdisks on MSA 2012 | For MSA 2012 Dual Controller Array configuration: <ol style="list-style-type: none"> Navigate to Manage > Volume Management > Delete Volume and select the volume to delete. Repeat for all volumes. Navigate to Virtual Disk Config > Delete a vdisk and select the vdisk to delete. Repeat for all vdisks. Navigate to Virtual Disk Config > Global Spares Menu > Delete Global Spares. Select all of the global spare disks and click Delete Global Spares. Repeat this step for second controller. |
| 4. <input type="checkbox"/> | Fibre Channel Controller GUI: Delete volumes and vdisks on P2000 | For P2000 MSA Dual Controller Array configuration: <ol style="list-style-type: none"> Navigate to Provisioning > Delete Volumes and select all volumes to delete. Navigate to Provisioning > Delete vdisks and select all vdisks to delete. Navigate to Provisioning > Manage Global Spares, unselect all the global spare disks, and click Modify Spares. Repeat this step for second controller. |
| 5. <input type="checkbox"/> | OA GUI: Login | Navigate to the IP address of the active OA, using Appendix C Determine which Onboard Administrator is Active. Login as an administrator. |

Procedure 93. Remove SAN Volume from Blade Server Without Preserving Existing TPD Installation

| Step | Procedure | Results |
|--------------------------------|--|--|
| 6. <input type="checkbox"/> | OA GUI: Delete zones from Brocade switches | <ol style="list-style-type: none"> 1. Select one of the Brocade switches and click Management Console. 2. Login as an administrative user. 3. Select Zone Admin and click Clear All. Wait for success message in bottom left of window and Effective zone Config: Default, All Access in bottom right of window. 4. Click Save Config. 5. Repeat for the second switch. |
| 7. <input type="checkbox"/> | Run IPM on blade server | <p>Run IPM on blade servers 9.9 IPM Servers Using PMAC Application.</p> <p>Note: A new IP address is assigned to bond0 of each blade at the end of the IPM process, so the XML files need to be updated accordingly.</p> |

11. Virtualization Procedures

11.1 Create Guest Server Using PMAC Application

This procedure creates a virtualized guest server on a TVOE host using the PMAC web GUI.

Prerequisites:

- Enclosure containing the TVOE host blade server to host the guest has been configured using 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- The TVOE host has been installed using 9.9 IPM Servers Using PMAC Application.

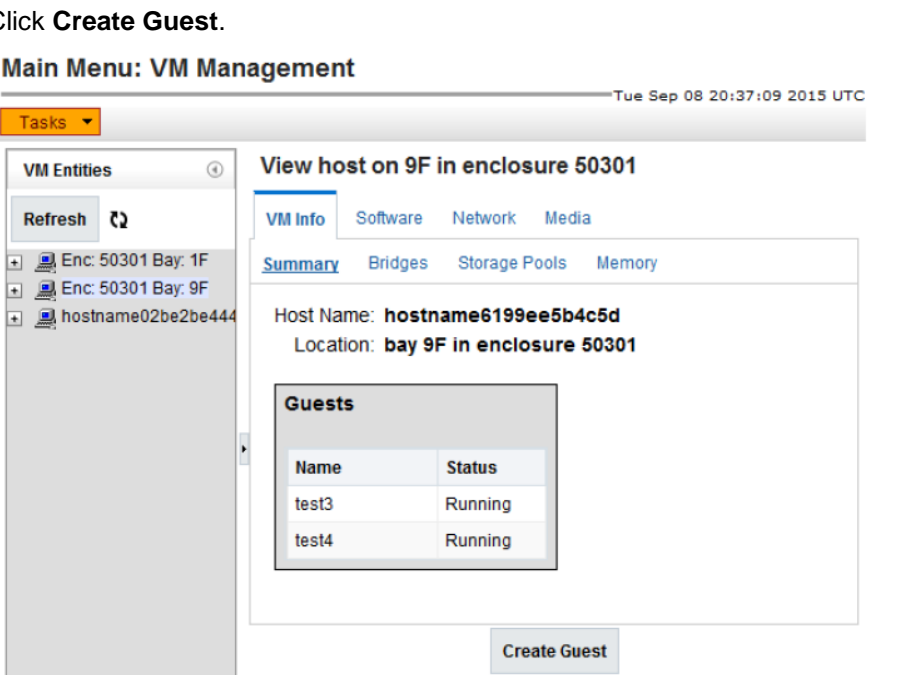
Note: PMAC does not prevent over-subscription of memory or CPU resources.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 94. Create Guest Server Using PMAC Application

| Step | Procedure | Results |
|--------------------------------|---------------------------|--|
| 1. <input type="checkbox"/> | PMAC GUI: Login | <p>Open a web browser and type:</p> <p><code>https://<pmac_management_network_IP></code></p> <p>Login as guiadmin user.</p> |
| 2. <input type="checkbox"/> | PMAC GUI | Navigate to Main Menu > VM Management . |

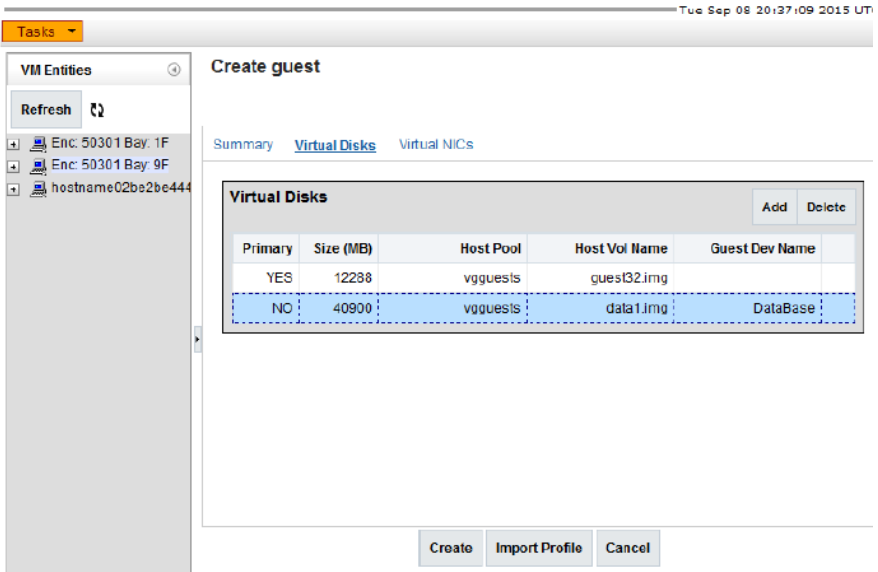
Procedure 94. Create Guest Server Using PMAC Application

| Step | Procedure | Results |
|---|------------------------|--|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI</p> | <p>Click Create Guest.</p>  |

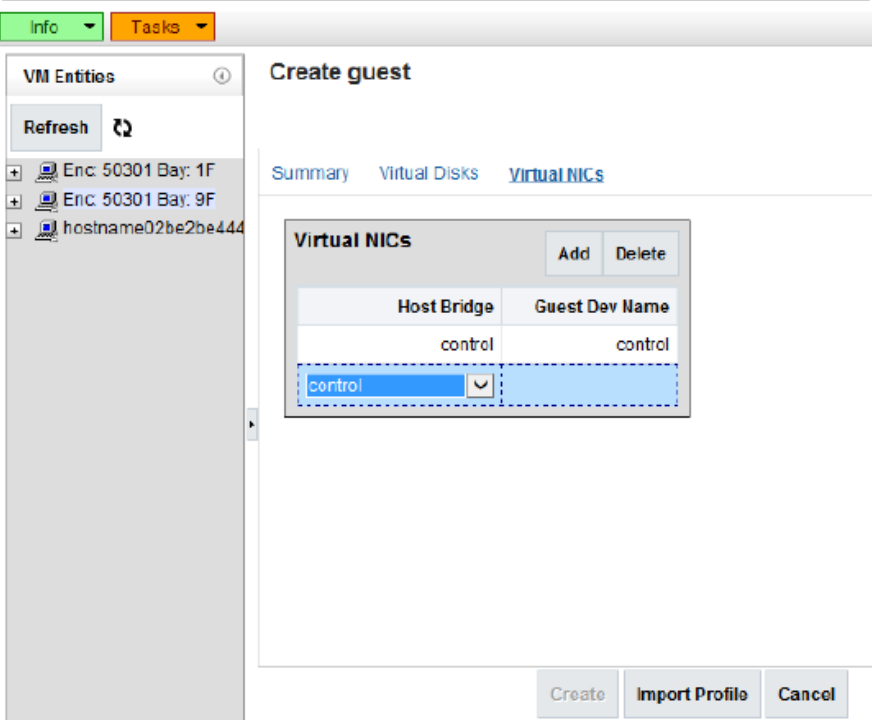
Procedure 94. Create Guest Server Using PMAC Application

| Step | Procedure | Results |
|-----------|------------------------|---|
| <p>4.</p> | <p>PMAC GUI</p> | <ol style="list-style-type: none"> Type a Name (something unique to the TVOE host). The name can be identical to a guest on a different host. From the Host options, select the TVOE host on which to create the guest. <p>Main Menu: VM Management</p> <p style="text-align: right;">Tue Sep 08 20:37:09 2015 UT</p> <p>Tasks ▾</p> <div style="display: flex;"> <div style="border: 1px solid gray; padding: 5px; width: 30%;"> <p>VM Entities</p> <p>Refresh ↻</p> <ul style="list-style-type: none"> + Enc: 50301 Bay: 1F + Enc: 50301 Bay: 9F + hostname02be2be444 </div> <div style="width: 70%;"> <p>Create guest</p> <p>Summary Virtual Disks Virtual NICs</p> <hr/> <p>Set Power State: On ▾</p> <p>Guest Name (Required): <input type="text" value="guest32"/></p> <p>Host: Enc: 50301 Bay: 9F</p> <p>Number of vCPUs: <input type="text" value="1"/> ▾</p> <p>Memory (MBs): <input type="text" value="4096"/> ▾</p> <p style="text-align: right;">Available host memory: 125 MB</p> <p>VM UUID: <input type="text"/></p> <p>Enable Virtual Watchdog <input checked="" type="checkbox"/></p> <p style="text-align: right;"> <input type="button" value="Create"/> <input type="button" value="Import Profile"/> <input type="button" value="Cancel"/> </p> </div> </div> <ol style="list-style-type: none"> From the Set Power State options, select the initial power state for the guest. <p>In this context, Shutdown and Destroy both behave the same. The guest is not powered on upon creation.</p> <ol style="list-style-type: none"> Edit the vCPU count and Memory size. <p>Adjust the number of virtual CPUs and the amount of memory (in MBs) to use for the guest. These fields are also manually editable test fields. PMAC does not prevent over-subscription of these resources.</p> <ol style="list-style-type: none"> If this Guest is being created on a version of TVOE having support for virtual guest watchdogs, the Enable Virtual Watchdog checkbox displays. Set this checkbox according to whether or not watchdog support is desired for this guest. |

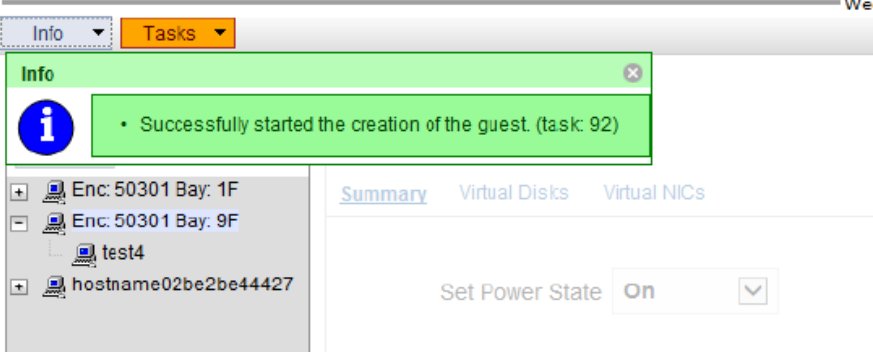
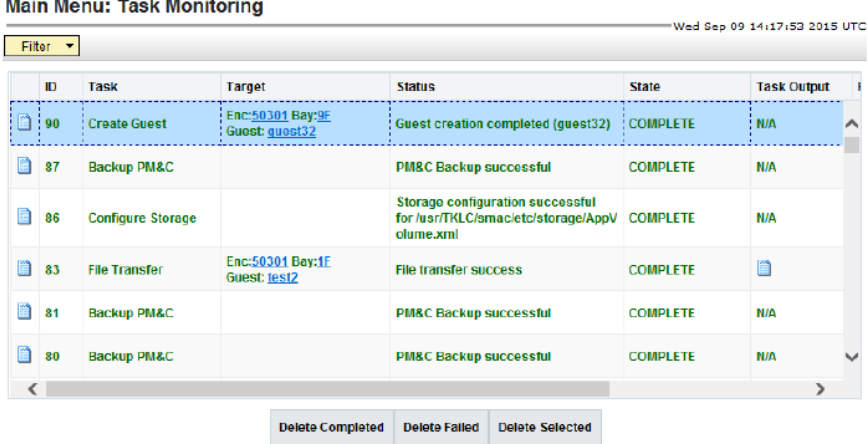
Procedure 94. Create Guest Server Using PMAC Application

| Step | Procedure | Results | | | | | | | | | | | | | | | |
|--|---|---|---------------|----------------|-----------|---------------|----------------|-----|-------|----------|-------------|--|----|-------|----------|-----------|----------|
| <p>5. <input type="checkbox"/></p> | <p>PMAC GUI: Edit the primary virtual disk</p> | <p>A primary disk is specified by default. The Virtual Disks list can be edited to change the details of the primary disk and to add virtual disks. The primary disk is used to install the OS. See the application requirements for the desired settings.</p> <p>Size (MB): By default, a primary disk is specified with the minimum size supported by TPD.</p> <p>Host Pool: The default vgguests storage pool is selected. Other pools that have been configured on the TVOE can be selected from the options.</p> <p>Host Vol Name: For the primary disk, this is filled in automatically based on the guest name provided. It can be modified manually if needed. It must be unique among all disks on all guests hosted on the TVOE.</p> <p>Guest Dev Name: For the primary disk, this value is not set. For added disks, this is the alias used inside the TPD instance running on the guest. It helps the application identify the disk.</p> <p>Click Add at the top-right corner of the Virtual Disks pane if the application requires extra virtual disks to be specified. Repeat for each extra disk.</p> <p>Main Menu: VM Management</p>  <p>Tue Sep 08 20:37:09 2015 UT</p> <p>Tasks</p> <p>VM Entities</p> <p>Refresh</p> <ul style="list-style-type: none"> Enc: 50301 Bay: 1F Enc: 50301 Bay: 9F hostname02be2be444 <p>Create guest</p> <p>Summary Virtual Disks Virtual NICs</p> <table border="1"> <thead> <tr> <th>Primary</th> <th>Size (MB)</th> <th>Host Pool</th> <th>Host Vol Name</th> <th>Guest Dev Name</th> </tr> </thead> <tbody> <tr> <td>YES</td> <td>12288</td> <td>vgguests</td> <td>guest32.img</td> <td></td> </tr> <tr> <td>NO</td> <td>40900</td> <td>vgguests</td> <td>data1.img</td> <td>DataBase</td> </tr> </tbody> </table> <p>Add Delete</p> <p>Create Import Profile Cancel</p> | Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | YES | 12288 | vgguests | guest32.img | | NO | 40900 | vgguests | data1.img | DataBase |
| Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | | | | | | | | | | | | | |
| YES | 12288 | vgguests | guest32.img | | | | | | | | | | | | | | |
| NO | 40900 | vgguests | data1.img | DataBase | | | | | | | | | | | | | |

Procedure 94. Create Guest Server Using PMAC Application

| Step | Procedure | Results |
|---|--|---|
| <p>6.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Add virtual NICs</p> | <p>By default, the control network is configured, and is required for PMAC to install and upgrade the guest. If this is removed, one is added during the guest creation.</p> <p>To add additional NICs, repeat this step for each virtual NIC.</p> <p>Click Add at the top-right corner of the Virtual NICs pane.</p> <p>Host Bridge: Select the desired bridge that has been previously configured on the TVOE.</p> <p>Guest Dev Name: This is the alias used inside of the TPD instance running on the guest. It helps the application identify the network.</p> <p>Main Menu: VM Management</p>  <p>Repeat as needed for each vNIC.</p> |

Procedure 94. Create Guest Server Using PMAC Application

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-----------------|--|--|--|----------|-------------|--------|-------|-------------|----|--------------|------------------------------------|------------------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------------|--|--|----------|-----|----|---------------|----------------------------------|-----------------------|----------|--|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|
| <p>7. □</p> | <p>PMAC GUI: Create the guest</p> | <p>Verify the guest configuration and click Create. If there was an immediate problem, an alert box displays to report the error, and the values can be corrected and retried. Otherwise, the Info box confirms the creation of a Background Task.</p> <p>Main Menu: VM Management</p>  <p>The screenshot shows the 'Main Menu: VM Management' interface. At the top, there are 'Info' and 'Tasks' dropdown menus. A green 'Info' box displays the message: 'Successfully started the creation of the guest. (task: 92)'. Below this, a list of VMs is shown with expandable/collapsible icons: 'Enc: 50301 Bay: 1F', 'Enc: 50301 Bay: 9F', 'test4', and 'hostname02be2be44427'. On the right, there are tabs for 'Summary', 'Virtual Disks', and 'Virtual NICs', and a 'Set Power State' dropdown menu currently set to 'On'.</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>8. □</p> | <p>PMAC GUI: Monitor guest create</p> | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the VirtAction: Create background task.</p> <p>Main Menu: Task Monitoring</p>  <p>The screenshot shows the 'Main Menu: Task Monitoring' interface. It features a 'Filter' dropdown and a timestamp 'Wed Sep 09 14:17:52 2015 UTC'. Below is a table with the following data:</p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Task Output</th> </tr> </thead> <tbody> <tr> <td>90</td> <td>Create Guest</td> <td>Enc:50301 Bay:9F Guest: guest32</td> <td>Guest creation completed (guest32)</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>87</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>86</td> <td>Configure Storage</td> <td></td> <td>Storage configuration successful for /usr/TKLC/smac/etc/storage/AppV olume.xml</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>83</td> <td>File Transfer</td> <td>Enc:50301 Bay:1F Guest: test4</td> <td>File transfer success</td> <td>COMPLETE</td> <td></td> </tr> <tr> <td>81</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>80</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> </tbody> </table> <p>At the bottom of the table, there are buttons for 'Delete Completed', 'Delete Failed', and 'Delete Selected'.</p> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> | ID | Task | Target | Status | State | Task Output | 90 | Create Guest | Enc:50301 Bay:9F Guest: guest32 | Guest creation completed (guest32) | COMPLETE | N/A | 87 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 86 | Configure Storage | | Storage configuration successful for /usr/TKLC/smac/etc/storage/AppV olume.xml | COMPLETE | N/A | 83 | File Transfer | Enc:50301 Bay:1F Guest: test4 | File transfer success | COMPLETE | | 81 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 80 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A |
| ID | Task | Target | Status | State | Task Output | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 90 | Create Guest | Enc:50301 Bay:9F Guest: guest32 | Guest creation completed (guest32) | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 87 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 86 | Configure Storage | | Storage configuration successful for /usr/TKLC/smac/etc/storage/AppV olume.xml | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 83 | File Transfer | Enc:50301 Bay:1F Guest: test4 | File transfer success | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 81 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

11.2 Delete Guest Server Using PMAC Application

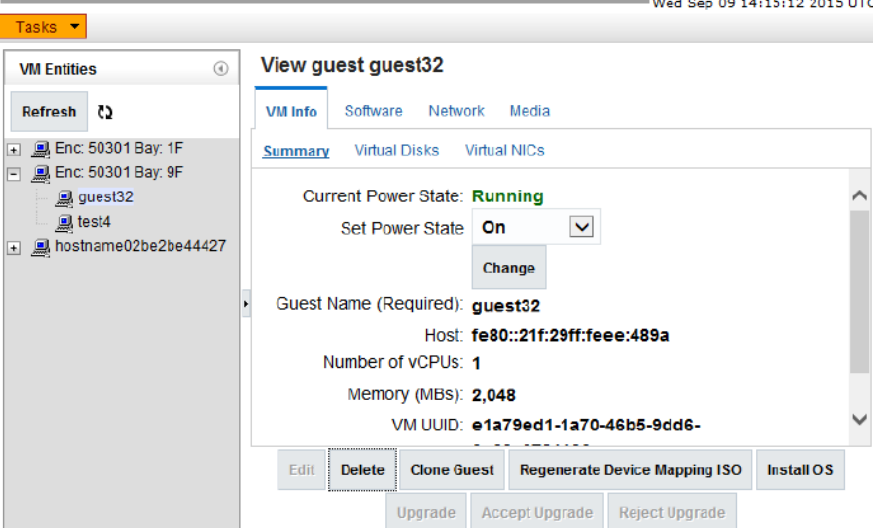
This procedure deletes a virtualized guest server on a TVOE host using the PMAC web GUI.

Prerequisite: Enclosure containing the TVOE host blade server to host the guest has been configured using 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.

Note: All data belonging to the guest server is lost in the execution of this procedure.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 95. Delete Guest Server Using PMAC Application

| Step | Procedure | Results |
|--------------------------------|---------------------------|---|
| 1. <input type="checkbox"/> | PMAC GUI: Login | Open a web browser and type: <code>https://<pmac_management_network_IP></code> Login as guiadmin user. |
| 2. <input type="checkbox"/> | PMAC GUI | Navigate to Main Menu > VM Management. |
| 3. <input type="checkbox"/> | PMAC GUI | <p>1. Click + to expand the TVOE host that contains the guest server to delete.</p> <p>2. Select the guest to delete.</p> <p>The guest details display on the right.</p> <p>Main Menu: VM Management</p>  <p>3. Click Delete.</p> <p>4. Click OK to confirm.</p> <p>Take a moment to double-check that the guest name is correct. There is no further confirmation and the delete is final.</p> |

Procedure 95. Delete Guest Server Using PMAC Application

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|--|---|--|----------|-------------|--------|-------|-------------|----|--------------|------------------------------------|------------------------------------|----------|-----|----|--------------|------------------------------------|------------------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------------|--|--|----------|-----|----|---------------|----------------------------------|-----------------------|----------|--|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|----|-------------|--|------------------------|----------|-----|
| 4. <input type="checkbox"/> | PMAC GUI: Monitor guest deletion | <p>Navigate to Main Menu > Task Monitoring to monitoring the VirtAction: Delete background task.</p> <p>Main Menu: Task Monitoring Wed Sep 09 14:32:19 2015 UTC</p> <p>Filter <input type="text"/></p> <table border="1"> <thead> <tr> <th>ID</th> <th>Task</th> <th>Target</th> <th>Status</th> <th>State</th> <th>Task Output</th> </tr> </thead> <tbody> <tr> <td>91</td> <td>Delete Guest</td> <td>Enc:50301 Bay:9F Guest: quest32</td> <td>Guest deletion completed (quest32)</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>90</td> <td>Create Guest</td> <td>Enc:50301 Bay:9F Guest: quest32</td> <td>Guest creation completed (quest32)</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>87</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>86</td> <td>Configure Storage</td> <td></td> <td>Storage configuration successful for /usr/TKLC/smacc/etc/storage/AppVolume.xml</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>83</td> <td>File Transfer</td> <td>Enc:50301 Bay:1F Guest: test2</td> <td>File transfer success</td> <td>COMPLETE</td> <td></td> </tr> <tr> <td>81</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>80</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>79</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> <tr> <td>78</td> <td>Backup PM&C</td> <td></td> <td>PM&C Backup successful</td> <td>COMPLETE</td> <td>N/A</td> </tr> </tbody> </table> <p style="text-align: center;"> <input type="button" value="Delete Completed"/> <input type="button" value="Delete Failed"/> <input type="button" value="Delete Selected"/> </p> <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> | ID | Task | Target | Status | State | Task Output | 91 | Delete Guest | Enc:50301 Bay:9F Guest: quest32 | Guest deletion completed (quest32) | COMPLETE | N/A | 90 | Create Guest | Enc:50301 Bay:9F Guest: quest32 | Guest creation completed (quest32) | COMPLETE | N/A | 87 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 86 | Configure Storage | | Storage configuration successful for /usr/TKLC/smacc/etc/storage/AppVolume.xml | COMPLETE | N/A | 83 | File Transfer | Enc:50301 Bay:1F Guest: test2 | File transfer success | COMPLETE | | 81 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 80 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 79 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | 78 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A |
| ID | Task | Target | Status | State | Task Output | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 91 | Delete Guest | Enc:50301 Bay:9F Guest: quest32 | Guest deletion completed (quest32) | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 90 | Create Guest | Enc:50301 Bay:9F Guest: quest32 | Guest creation completed (quest32) | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 87 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 86 | Configure Storage | | Storage configuration successful for /usr/TKLC/smacc/etc/storage/AppVolume.xml | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 83 | File Transfer | Enc:50301 Bay:1F Guest: test2 | File transfer success | COMPLETE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 81 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 80 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 79 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 78 | Backup PM&C | | PM&C Backup successful | COMPLETE | N/A | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

11.3 Create Guest Server from Guest Archive Using PMAC Application

This procedure creates virtualized guest server from a guest archive image on a TVOE host, using the PMAC web GUI.

Prerequisites:

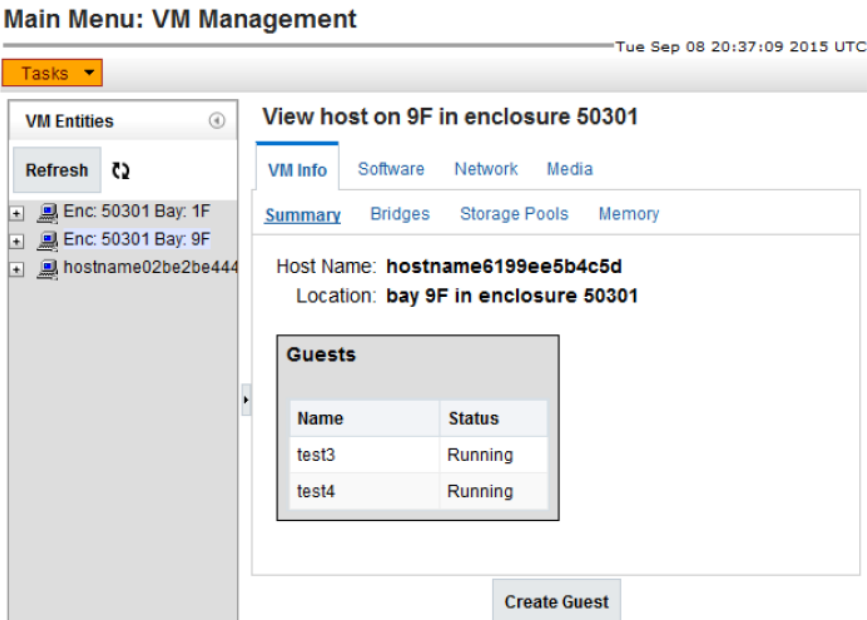
- Enclosure containing the TVOE host blade server to host the guest has been configured using 9.6 Add Cabinet and Enclosure to the PMAC System Inventory.
- The TVOE host has been installed using 9.9 IPM Servers Using PMAC Application.
- The ISO image providing the guest archive image and profile has been provisioned using 9.8 Add ISO Images to the PMAC Image Repository.

Notes:

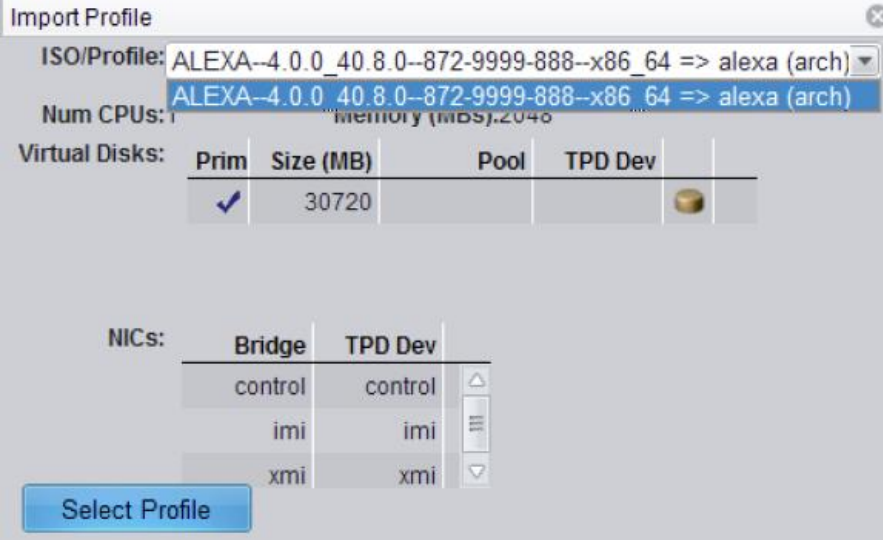
- PMAC does not prevent over-subscription of memory or CPU resources.
- The guest archive profiles might not contain values for all required fields.
- The values provided by the guest archive profile can be overridden before the guest is created.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 96. Create Guest Server from Guest Archive Using PMAC Application

| Step | Procedure | Results | | | | | | |
|--------------------------------|---------------------------|--|------|--------|-------|---------|-------|---------|
| 1. <input type="checkbox"/> | PMAC GUI: Login | Open a web browser and type: <code>https://<pmac_management_network_IP></code> Login as guiadmin user. | | | | | | |
| 2. <input type="checkbox"/> | PMAC GUI | Navigate to Main Menu > VM Management . | | | | | | |
| 3. <input type="checkbox"/> | PMAC GUI | <p>Click Create Guest.</p>  <p>Main Menu: VM Management Tue Sep 08 20:37:09 2015 UTC</p> <p>Tasks ▾</p> <p>VM Entities ⊙</p> <p>Refresh ↻</p> <ul style="list-style-type: none"> + Enc: 50301 Bay: 1F + Enc: 50301 Bay: 9F + hostname02be2be444 <p>View host on 9F in enclosure 50301</p> <p>VM Info Software Network Media</p> <p>Summary Bridges Storage Pools Memory</p> <p>Host Name: hostname6199ee5b4c5d Location: bay 9F in enclosure 50301</p> <p>Guests</p> <table border="1" data-bbox="792 976 1068 1092"> <thead> <tr> <th>Name</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>test3</td> <td>Running</td> </tr> <tr> <td>test4</td> <td>Running</td> </tr> </tbody> </table> <p style="text-align: right;">Create Guest</p> | Name | Status | test3 | Running | test4 | Running |
| Name | Status | | | | | | | |
| test3 | Running | | | | | | | |
| test4 | Running | | | | | | | |

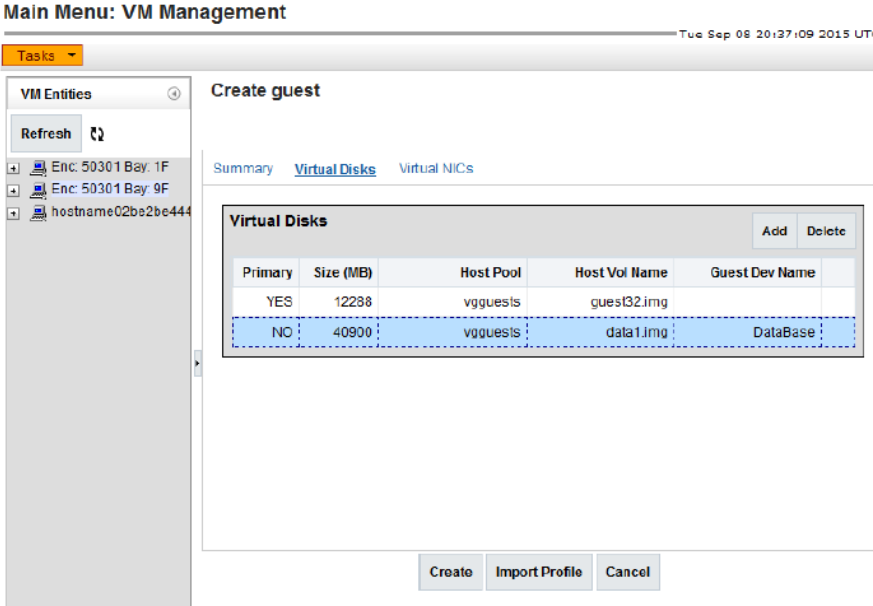
Procedure 96. Create Guest Server from Guest Archive Using PMAC Application

| Step | Procedure | Results |
|---|------------------------|---|
| <p>4.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI</p> | <p>Click Import Profile.</p> <p>Main Menu: VM Management</p> <p style="text-align: right;">Wed Sep 09 14:15:1</p> <p>Info Tasks</p> <div style="display: flex;"> <div style="flex: 1;"> <p>VM Entities</p> <p>Refresh</p> <ul style="list-style-type: none"> + Enc: 50301 Bay: 1F + Enc: 50301 Bay: 9F + hostname02be2be44427 </div> <div style="flex: 2;"> <p>Create guest</p> <p>Summary Virtual Disks Virtual NICs</p> <hr/> <p>Set Power State On</p> <p>Guest Name (Required): <input type="text"/></p> <p>Host: Enc: 50301 Bay: 9F</p> <p>Number of vCPUs: 1</p> <p>Memory (MBs): 4096</p> <p>Available host memory: 2173 MB</p> <p>VM UUID: <input type="text"/></p> <p>Enable Virtual Watchdog <input checked="" type="checkbox"/></p> <p style="text-align: right;">Create Import Profile Cancel</p> </div> </div> |
| <p>5.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI</p> | <p>Select the desired profile and click Select Profile.</p>  <p>There may be multiple profiles on an ISO. Verify the details.</p> |

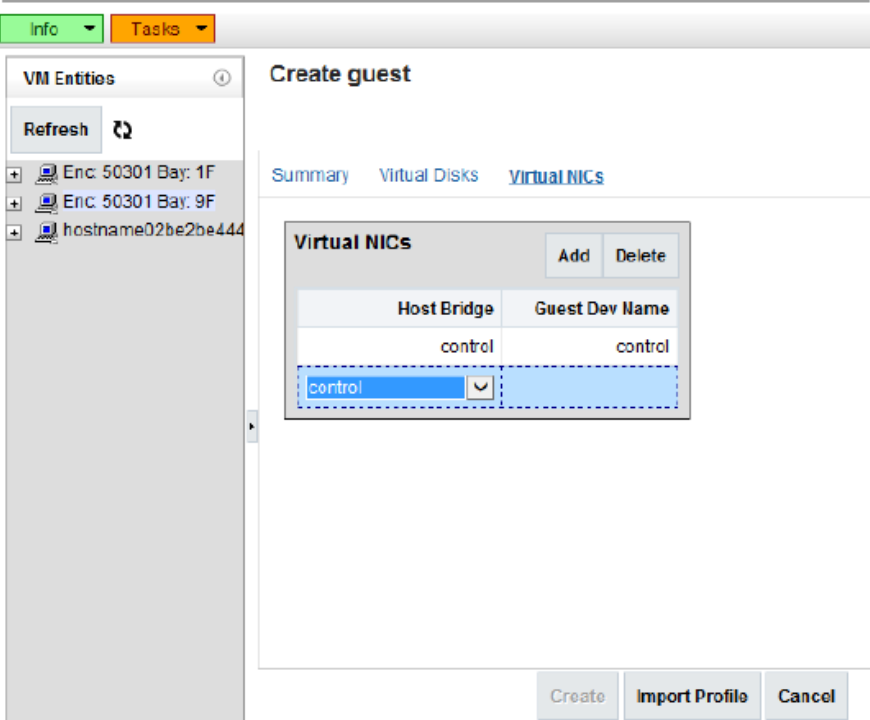
Procedure 96. Create Guest Server from Guest Archive Using PMAC Application

| Step | Procedure | Results |
|--|------------------------|--|
| <p>6. <input type="checkbox"/></p> | <p>PMAC GUI</p> | <ol style="list-style-type: none"> The profile fills in the default name. If a different name is desired, type a Name that is something unique to the TVOE host. The name can be identical to a guest on a different host. From the Host options, select the TVOE host on which to create the guest. <div style="margin-left: 20px;"> <p>Guest Name (Required): <input type="text" value="alexa1"/></p> <p>Host: <input type="text" value="Enc: 50301 Bay: 9F"/></p> <p>Number of vCPUs: <input type="text" value="hostname02be2be44427"/></p> <p>Memory (MBs): <input type="text" value="4096"/></p> </div> From the Set Power State options, select the initial power state for the guest. <p>In this context, Shutdown and Destroy both behave the same. The guest is not powered on upon creation.</p> Edit the vCPU count and Memory size. <p>Adjust the number of virtual CPUs and the amount of memory (in MBs) to use for the guest. These fields are also manually editable test fields. PMAC does not prevent over-subscription of these resources.</p> If this Guest is being created on a version of TVOE having support for virtual guest watchdogs, the Enable Virtual Watchdog checkbox displays. Set this checkbox according to whether or not watchdog support is desired for this guest. |

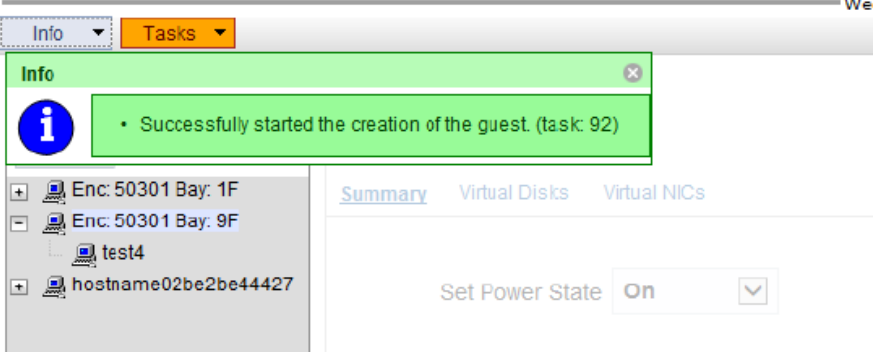
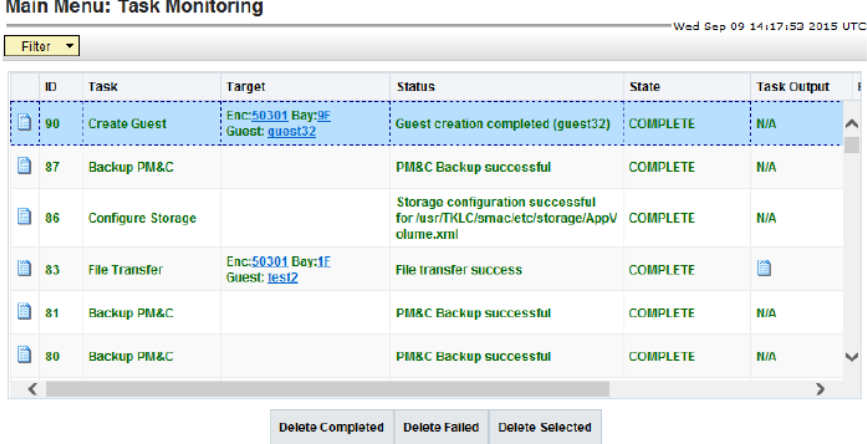
Procedure 96. Create Guest Server from Guest Archive Using PMAC Application

| Step | Procedure | Results | | | | | | | | | | | | | | | |
|--|---|---|---------------|----------------|-----------|---------------|----------------|-----|-------|----------|-------------|--|----|-------|----------|-----------|----------|
| <p>7. <input type="checkbox"/></p> | <p>PMAC GUI: Edit the primary virtual disk</p> | <p>A primary disk is specified by default. The disk image shows how the disk is populated with the archive's image. The only fields that should be modified are the Host Pool and Host Vol Name columns.</p> <p>Size (MB): By default, a primary disk is specified with the minimum size supported by TPD.</p> <p>Host Pool: The desired storage pool can be selected here. It is possible that the profile did not specify a value for the storage pool. The GUI does not allow you to continue until one is selected. When adding a new disk, the default vgguests storage pool is selected.</p> <p>Host Vol Name: For the primary disk, this is filled in automatically based on the guest name provided. It can be modified manually if needed. It must be unique among all disks on all guests hosted on the TVOE.</p> <p>Guest Dev Name: For the primary disk, this value is not set. For added disks, this is the alias used inside the TPD instance running on the guest. It helps the application identify the disk.</p> <p>Click Add at the top-right corner of the Virtual Disks pane if the application requires extra virtual disks to be specified. Repeat for each extra disk.</p> <p>Main Menu: VM Management</p>  <p>The screenshot shows the 'Create guest' interface. On the left, there's a 'VM Entities' sidebar with a 'Refresh' button and a list of entities: 'Enc: 50301 Bay: 1F', 'Enc: 50301 Bay: 9F', and 'hostname02be2be444'. The main area is titled 'Create guest' and has tabs for 'Summary', 'Virtual Disks', and 'Virtual NICs'. The 'Virtual Disks' tab is selected, displaying a table with the following data:</p> <table border="1" data-bbox="737 1079 1373 1230"> <thead> <tr> <th>Primary</th> <th>Size (MB)</th> <th>Host Pool</th> <th>Host Vol Name</th> <th>Guest Dev Name</th> </tr> </thead> <tbody> <tr> <td>YES</td> <td>12288</td> <td>vgguests</td> <td>guest32.img</td> <td></td> </tr> <tr> <td>NO</td> <td>40900</td> <td>vgguests</td> <td>data1.img</td> <td>DataBase</td> </tr> </tbody> </table> <p>At the bottom of the 'Virtual Disks' pane, there are 'Add' and 'Delete' buttons. Below the table, there are 'Create', 'Import Profile', and 'Cancel' buttons.</p> | Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | YES | 12288 | vgguests | guest32.img | | NO | 40900 | vgguests | data1.img | DataBase |
| Primary | Size (MB) | Host Pool | Host Vol Name | Guest Dev Name | | | | | | | | | | | | | |
| YES | 12288 | vgguests | guest32.img | | | | | | | | | | | | | | |
| NO | 40900 | vgguests | data1.img | DataBase | | | | | | | | | | | | | |

Procedure 96. Create Guest Server from Guest Archive Using PMAC Application

| Step | Procedure | Results |
|---|---|---|
| <p>8.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Edit virtual NICs</p> | <p>By default, the control network is configured, and is required for PMAC to install and upgrade the guest. If this is removed, one is added during the guest creation.</p> <p>To add additional NICs, repeat this step for each virtual NIC.</p> <p>Click Add at the top-right corner of the Virtual NICs pane.</p> <p>Host Bridge: Select the desired bridge that has been previously configured on the TVOE.</p> <p>Guest Dev Name: This is the alias used inside of the TPD instance running on the guest. It helps the application identify the network.</p> <p>Main Menu: VM Management</p>  <p>Repeat as needed for each vNIC.</p> |

Procedure 96. Create Guest Server from Guest Archive Using PMAC Application

| Step | Procedure | Results |
|--|--|--|
| <p>9.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Create the guest</p> | <p>Verify the guest configuration and click Create.</p> <p>If there was an immediate problem, an alert box displays to report the error, and the values can be corrected and retried. Otherwise, the Info box confirms the creation of a Background Task.</p> <p>Main Menu: VM Management</p>  |
| <p>10.</p> <p><input type="checkbox"/></p> | <p>PMAC GUI: Monitor guest create</p> | <p>Navigate to Main Menu > Task Monitoring to monitor the progress of the VirtAction: Create background task.</p> <p>Main Menu: Task Monitoring</p>  <p>When the task is complete, the text changes to green and the Progress column indicates 100%.</p> |

12. General TPD-Based Application Procedures

12.1 Back Up TVOE

This procedure backs up system files to use when restoring a failed system.

Note: The backup image is stored on a customer provided medium.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 97. Back Up TVOE

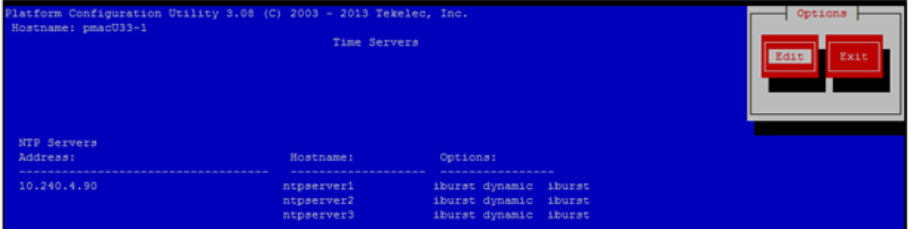
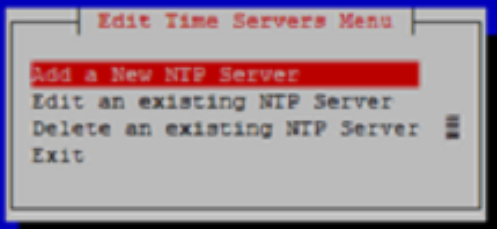
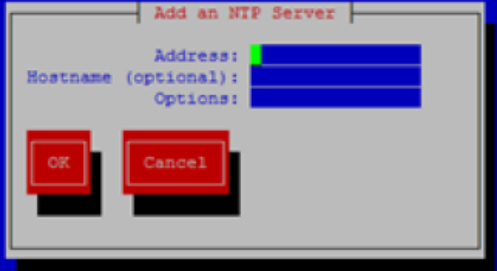
| Step | Procedure | Results |
|--------------------------------|------------------------------------|--|
| 1. <input type="checkbox"/> | TVOE Host: Login | Login as the platcfg user. |
| 2. <input type="checkbox"/> | TVOE Host: Back up files | <ol style="list-style-type: none"> Navigate to Maintenance > Backup and Restore > Backup Platform. Note: If this operation is attempted on a system without media (for example, the CD/DVD), a No disk device available. This is normal on systems without a CD ROM device message displays. Ignore the message and press any key to continue. Click Build ISO file only. The Creating ISO Image. . . message may display. After the ISO is created, platcfg returns to the Backup TekServer Menu screen. The ISO has now been created and is located in the /var/TKLC/bkp/ directory. An example filename of a backup file created is hostname1307466752-plat-app-201104171705.iso. Click Exit on each menu until platcfg exits. The SSH connection to the TVOE server terminates. Log into the customer server and copy the backup image to the customer server where it can be safely stored. If the customer system is a Linux system, execute the following command to copy the backup image to the customer system. <pre># scp tvoexfer@<TVOE IP Address>:/var/TKLC/bkp/* /path/to/destination/</pre> When prompted, enter the tvoexfer user password and press Enter. <pre># scp tvoexfer@<TVOE IP Address>:/var/TKLC/bkp/* /path/to/destination/ tvoexfer@10.24.34.73's password: hostname1301859532-plat-app-301104171705.iso 100% 134MB 26.9MB/s 00:05</pre> If the customer system is a Windows system, refer to Appendix A Using WinSCP to copy the backup image to the customer system. |

12.2 Configure NTP on TPD-Based Application

This procedure configures NTP servers for a server based on TPD.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 98. Configure NTP on TPD-Based Application

| Step | Results |
|------------------------------------|--|
| <p>1.</p> <input type="checkbox"/> | <p>Login as the platcfg user on the server.</p> |
| <p>2.</p> <input type="checkbox"/> | <p>Navigate to Network Configuration > NTP.</p>  |
| <p>3.</p> <input type="checkbox"/> | <p>Click Edit.</p>  |
| <p>4.</p> <input type="checkbox"/> | <p>Add, edit, and delete NTP servers as needed. Remember that three (3) NTP sources are required.</p> <p>Add an NTP server</p> <ol style="list-style-type: none"> 1. Click Add a New NTP Server. 2. Type the Address, Hostname (optional), Options. 3. Click OK.  <p>Edit an NTP server</p> <ol style="list-style-type: none"> 1. Click Edit an Existing NTP Server. 2. Select the NTP server. |

Procedure 98. Configure NTP on TPD-Based Application

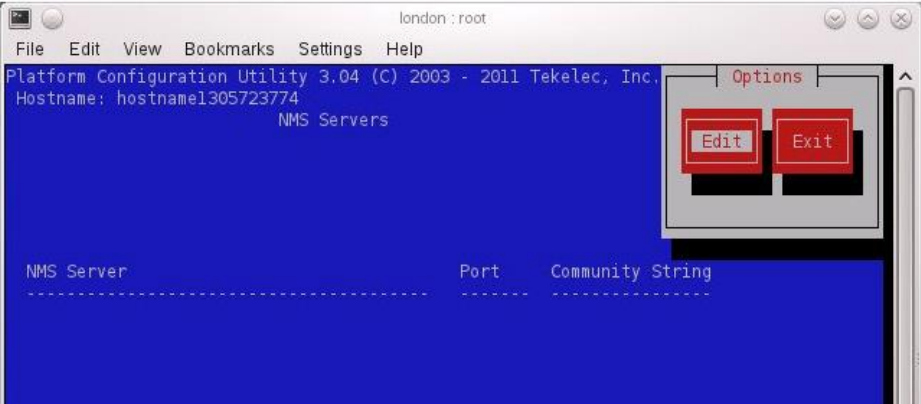
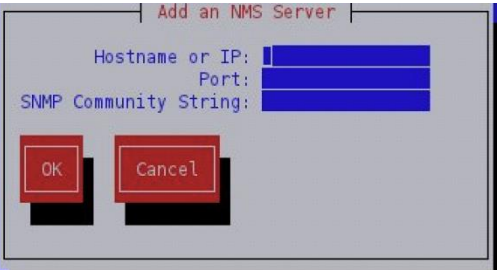
| Step | Results |
|--|--|
| | <div data-bbox="289 298 782 621" data-label="Image"> </div> <p data-bbox="289 630 938 705"> 3. Edit the Address, Hostname (optional), Options. 4. Click OK. </p> <div data-bbox="289 722 782 991" data-label="Image"> </div> <p data-bbox="289 999 555 1024">Delete an NTP server</p> <p data-bbox="289 1037 805 1113"> 1. Click Delete an existing NTP Server. 2. Select the NTP server and press Enter. </p> <div data-bbox="289 1129 782 1453" data-label="Image"> </div> <p data-bbox="289 1461 867 1495">3. Click Yes to confirm deleting the NTP server.</p> |
| <p data-bbox="207 1528 815 1558">5. <input type="checkbox"/> Click Exit and Yes to restart the NTP server.</p> | <div data-bbox="289 1566 782 1768" data-label="Image"> </div> |
| <p data-bbox="207 1793 792 1822">6. <input type="checkbox"/> Click Exit on each menu until platcfg exits.</p> | |

12.3 Add SNMP Trap Destination on TPD-Based Application

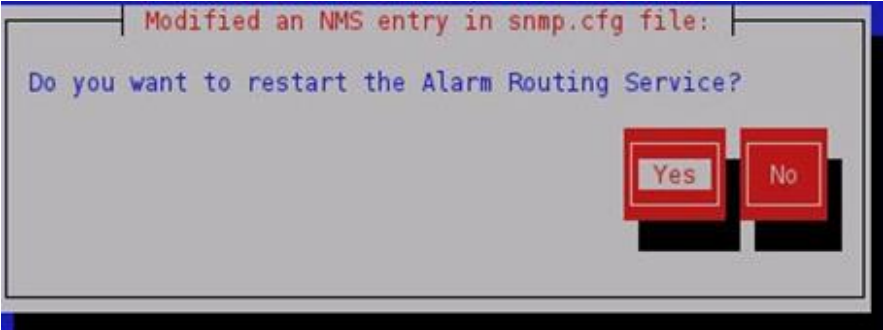
This procedure adds an SNMP trap destination to a server based on TPD. All alarm information is then sent to the NMS located at the destination.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 99. Add SNMP Trap Destination on TPD-Based Application

| Step | Results |
|--------------------------------|--|
| 1. <input type="checkbox"/> | Login as the platcfg user on the server. |
| 2. <input type="checkbox"/> | Navigate to Network Configuration > SNMP Configuration > NMS Configuration.  |
| 3. <input type="checkbox"/> | Click Edit . |
| 4. <input type="checkbox"/> | Click Add a New NMS Server . |
| 5. <input type="checkbox"/> | Type the information related to SNMP trap destination and click OK .  |

Procedure 99. Add SNMP Trap Destination on TPD-Based Application

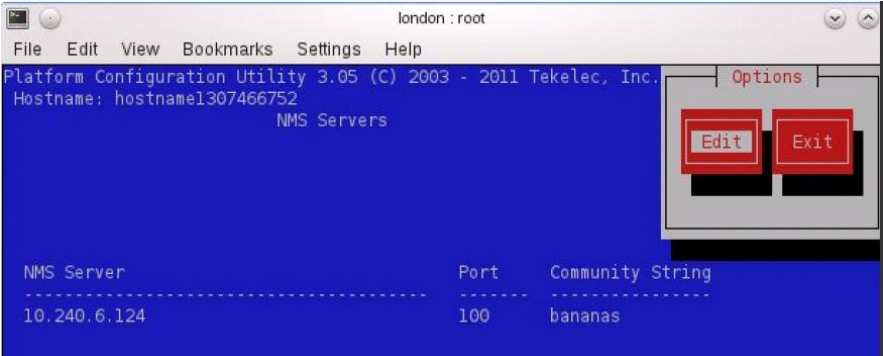
| Step | Results |
|--------------------------------|--|
| 6. <input type="checkbox"/> | Click Exit and Yes to restart the service.  |
| 7. <input type="checkbox"/> | Click Exit on each menu until platcfg exits. |

12.4 Delete SNMP Trap Destination on TPD-Based Application

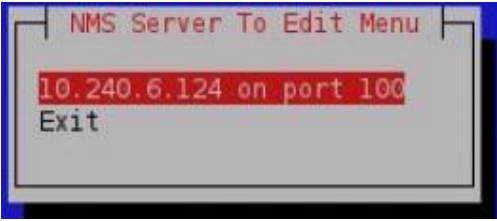
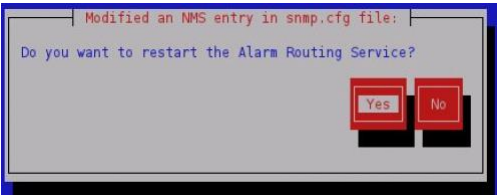
This procedure removes an SNMP trap destination on a server.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 100.Delete SNMP Trap Destination on TPD-Based Application

| Step | Results |
|--------------------------------|--|
| 1. <input type="checkbox"/> | Login as the platcfg user on the server. |
| 2. <input type="checkbox"/> | Navigate to Network Configuration > SNMP Configuration > NMS Configuration.  |
| 3. <input type="checkbox"/> | Click Edit . |
| 4. <input type="checkbox"/> | Click Delete an Existing NMS Server . |

Procedure 100.Delete SNMP Trap Destination on TPD-Based Application

| Step | Results |
|---|--|
| <p>5.</p> <p><input type="checkbox"/></p> | <p>Select the NMS server and press Enter.</p>  <p>Click Yes to confirm deleting the NMS server.</p> |
| <p>6.</p> <p><input type="checkbox"/></p> | <p>Click Exit and Yes to restart the service.</p>  |
| <p>7.</p> <p><input type="checkbox"/></p> | <p>Click Exit on each menu until platcfg exits.</p> |

12.5 Install the NetBackup Client Application

This procedure installs or upgrades the NetBackup client software on an application server.

NetBackup is a utility that allows for management of backups and recovery of remote systems. The NetBackup suite supports disaster recovery at the customer site.

Prerequisites:

- Application server platform installation has been completed.
- NAPD has been completed 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.
- 12.11 Create LV and Filesystem for NetBackup Client Software.

Note: For the PMAC application deployed with NetBackup Volume option `--netbackupVol` the guest virtual disk is created by deploy.

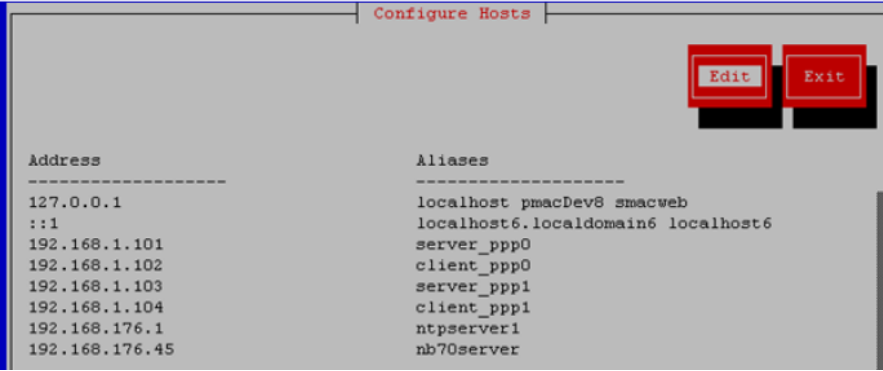
- Config file has been created if the version of NetBackup Client is not supported 12.13 Create NetBackup Client Config File.

Notes:

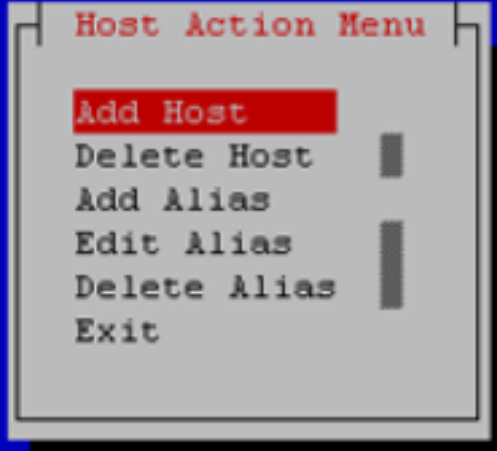
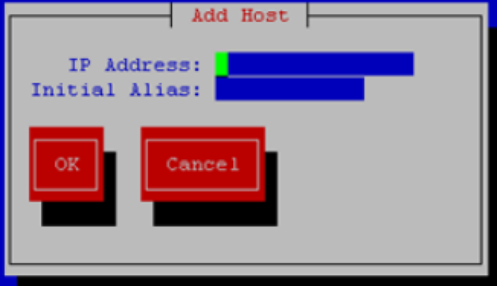
- Platform 7.6.x supports NetBackup 7.1, 7.5, and 7.6.x clients. If the NetBackup Client being installed is not supported, contact **Error! Bookmark not defined.** for guidance on creating a config file that allows for installation of unknown NetBackup Clients. 12.13 Create NetBackup Client Config File can be used once the contents of the config are known.
- Failure to install the NetBackup Client properly (that is, by neglecting to execute this procedure) may result in the NetBackup Client being deleted during an Oracle software upgrade.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 101. Install the NetBackup Client Application

| Step | Procedure | Results |
|--|--|---|
| <p>1. <input type="checkbox"/></p> | <p>Select and perform a NetBackup client installation path</p> | <p>There are two methods to install NetBackup Client.</p> <ul style="list-style-type: none"> • If a customer has a way of transferring and installing the NetBackup client without the aid of TPD tools, then use Netbackup Client Install with nbAutoInstall. This is not common and if the answer is not known then do not use Netbackup Client Install with nbAutoInstall. • If you do not use Netbackup Client Install with nbAutoInstall, use NetBackup Client Install/Upgrade with platcfg. |
| <p>2. <input type="checkbox"/></p> | <p>Application Console: Modify the hosts file</p> | <p>1. Use platform configuration utility (platcfg) to modify the hosts file with NetBackup server alias.</p> <p>Note: If NetBackup Client has successfully been installed, then you can find the NetBackup server's hostname in the /usr/opensv/netbackup/bp.conf file. It is identified by the SERVER configuration parameter as is shown in the following output:</p> <p>List NetBackup servers hostname:</p> <pre>\$ sudo cat /usr/opensv/netbackup/bp.conf SERVER = NB76Server CLIENT_NAME = 10.240.117.134 CONNECT_OPTIONS = localhost 1 0 2</pre> <p>Note: In the case of nbAutoInstall, the NetBackup client may not yet be installed. For this situation, the /usr/opensv/netbackup/bp.conf cannot be used to find the NetBackup server alias.</p> <p>2. Use platform configuration utility (platcfg) to update application hosts file with NetBackup Server alias.</p> <pre>\$ sudo su - platcfg</pre> <p>a. Navigate to Network Configuration > Modify Hosts File.</p> <p>b. Click Edit.</p>  <p>c. Click Add Host.</p> |

Procedure 101. Install the NetBackup Client Application

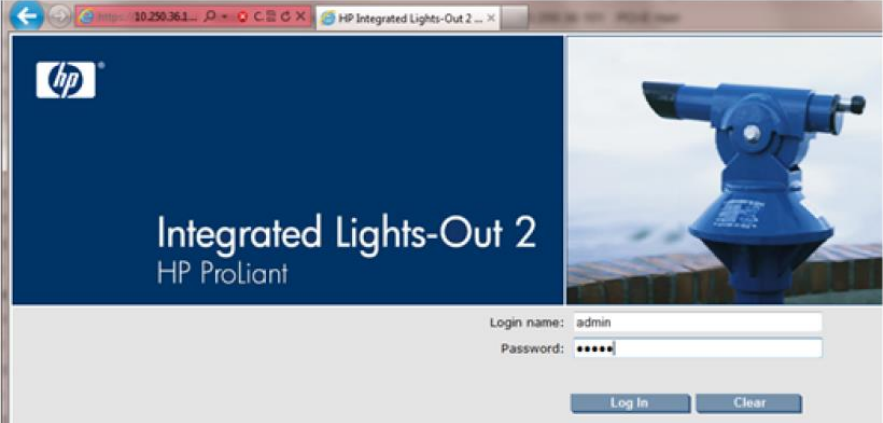
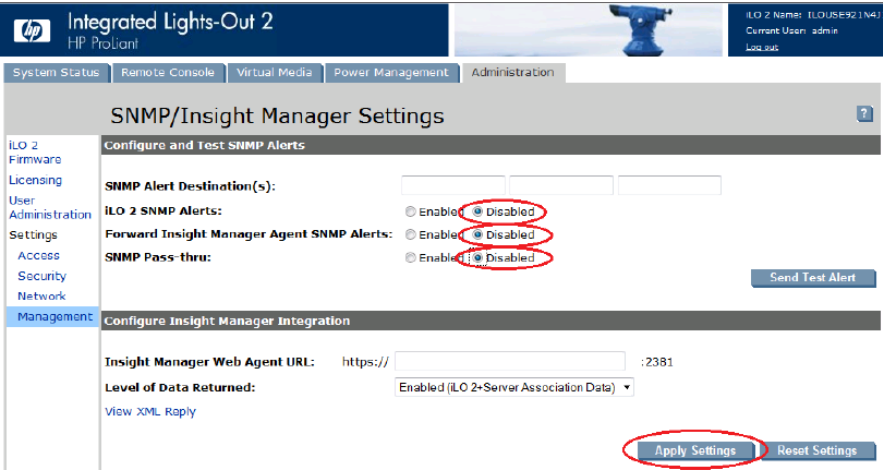
| Step | Procedure | Results |
|--|---|---|
| | |  <p>d. Type information and click OK.</p>  <p>e. Click Exit on each menu until platcfg exits.</p> |
| <p>3. <input type="checkbox"/></p> | <p>Application Console: Create to server</p> | <p>Create a link for the application provided NetBackup client notify scripts to path on application server where NetBackup expects to find them.</p> <p>Note: Link notify scripts from appropriate path on application server for given application.</p> <pre>\$ sudo mkdir -p /usr/opensv/netbackup/bin/ \$ sudo ln -s <path>/bpstart_notify /usr/opensv/netbackup/bin/bpstart_notify \$ sudo ln -s <path>/bpend_notify /usr/opensv/netbackup/bin/bpend_notify</pre> |

12.6 Change SNMP Configuration Settings for iLO2

This procedure changes the default SNMP settings for HP ProLiant iLO2 devices. Perform this procedure for every HP ProLiant G1/G5/G6 blade and rack mount server on the network

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 102. Change SNMP Configuration Settings for iLO2

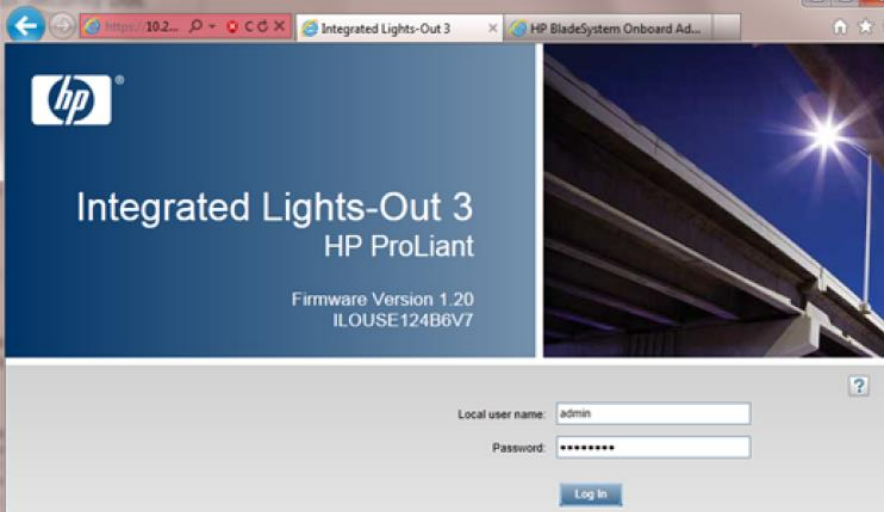
| Step | Procedure | Results |
|------------------------------------|---|---|
| <p>1. <input type="checkbox"/></p> | <p>iLO Web UI: Login</p> | <p>1. Open a web browser and navigate to the IP address of the iLO device. 2. Click Continue to this website (not recommended) if prompted. 3. Login using an account with administrative level privileges.</p>  |
| <p>2. <input type="checkbox"/></p> | <p>iLO Web UI: Management screen</p> | <p>1. Navigate to Administration > Management. 2. Select Disabled for each of the three SNMP alerts. 3. Click Apply Settings.</p>  |
| <p>3. <input type="checkbox"/></p> | <p>iLO Web UI: Verify settings</p> | <p>Navigate away from the SNMP Management page and then back to make sure the settings are correct. Click Log Out.</p> |
| <p>4. <input type="checkbox"/></p> | <p>Repeat</p> | <p>Repeat for each iLO2 device on the network.</p> |

12.7 Change SNMP Configuration Settings for iLO3 and iLO4

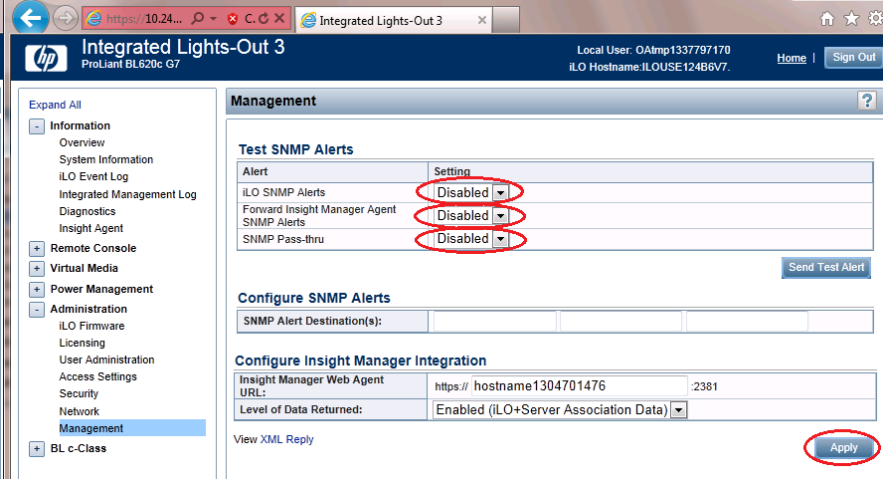
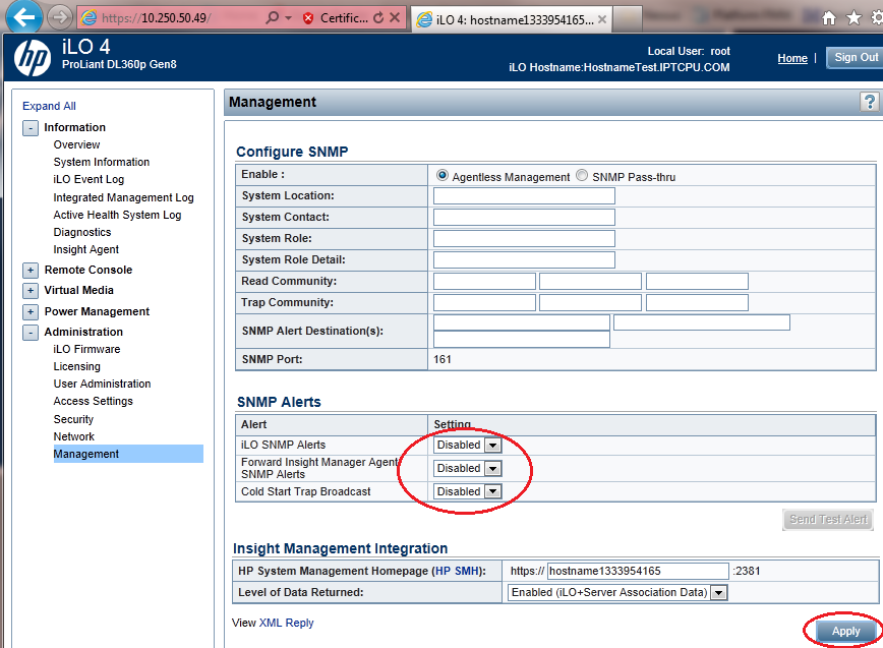
This procedure changes the default SNMP settings for HP ProLiant iLO3 devices. Perform this procedure for every HP ProLiant G7 blade and rack mount server on the network.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 103.Change SNMP Configuration Settings for iLO3 and iLO4

| Step | Procedure | Results |
|--------------------------------|-----------------------------|---|
| 1. <input type="checkbox"/> | iLO Web UI: Login | <ol style="list-style-type: none"> 1. Open a web browser and navigate to the IP address of the iLO device. 2. Click Continue to this website (not recommended) if prompted. 3. Login using an account with administrative level privileges.  |

Procedure 103. Change SNMP Configuration Settings for iLO3 and iLO4


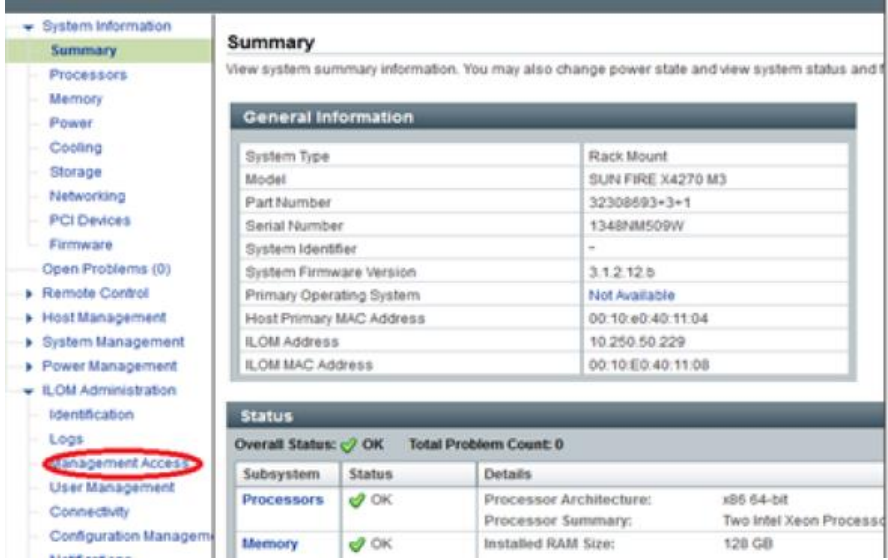
| Step | Procedure | Results |
|---|---|--|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>iLO Web UI: Management screen</p> | <p>1. Navigate to Administration > Management.</p> <p>2. Select Disabled for each of the three SNMP alerts.</p> <p>3. Click Apply.</p> <p>iLO3 Web UI:</p>  <p>iLO4 Web UI:</p>  |
| <p>3.</p> <p><input type="checkbox"/></p> | <p>iLO Web UI: Verify settings</p> | <p>Navigate away from the SNMP Management page and then back to make sure the settings are correct.</p> <p>Click Sign Out.</p> |
| <p>4.</p> <p><input type="checkbox"/></p> | <p>Repeat</p> | <p>Repeat for each iLO3 and iLO4 device on the network.</p> |

12.8 Change SNMP Configuration Settings for iLOM

This procedure changes the default SNMP settings for ILOM devices. Perform this procedure for every ILOM device on the network.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 104.Change SNMP Configuration Settings for iLOM

| Step | Procedure | Results |
|------------------------------------|---|--|
| <p>1. <input type="checkbox"/></p> | <p>ILOM Web UI: Login</p> | <ol style="list-style-type: none"> Open a web browser and navigate to the IP address of the ILOM device. Click Continue to this website (not recommended) if prompted. Login using an account with administrative level privileges.  |
| <p>2. <input type="checkbox"/></p> | <p>ILOM Web UI: Management Access screen</p> | <ol style="list-style-type: none"> Navigate to System Information > Summary. Click Management Access.  <ol style="list-style-type: none"> Click the SNMP tab. Unmark the Enabled checkbox. Click Save. |

12.9 Install NetBackup Client with nbAutoInstall

This procedure enables TPD to detect automatically when a NetBackup client is installed and completes TPD-related tasks needed for effective NetBackup client operation. With this procedure, the NetBackup client install (pushing the client and performing the install) is the responsibility of the customer and is not covered in this procedure.

Notes:

- If the customer does not have a way to push and install the NetBackup client, then use 12.10 Install/Upgrade NetBackup Client with platcfg.
- This procedure must be executed before the customer does the NetBackup client install.

Prerequisites:

- Application server platform installation has been completed.
- NAPD has been completed 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.
- Filesystem for NetBackup client software has been created using 12.11 Create LV and Filesystem for NetBackup Client Software.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 105.Install NetBackup Client with nbAutoInstall

| Step | Results |
|--------------------------------|--|
| 1. <input type="checkbox"/> | Complete workaround to prepare the server, if workaround is required as directed by Error! Bookmark not defined. |
| 2. <input type="checkbox"/> | Enable nbAutoInstall. <pre>\$ sudo /usr/TKLC/plat/bin/nbAutoInstall --enable</pre> The server periodically checks if a new version of the NetBackup client has been installed and performs necessary TPD configuration accordingly. At any time, you can now push and install a new version of the NetBackup Client. |

12.10 Install/Upgrade NetBackup Client with platcfg

This procedure pushes and installs NetBackup client using platcfg menus.

Prerequisites:

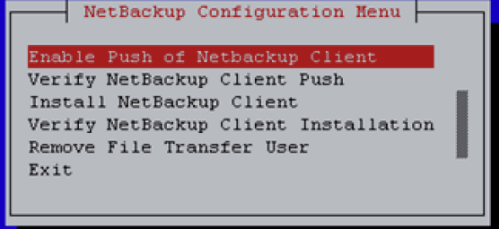
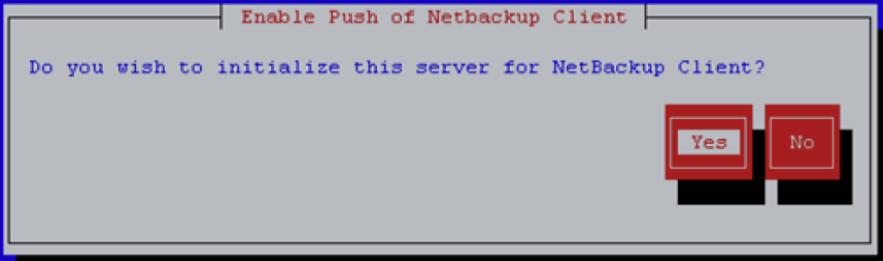
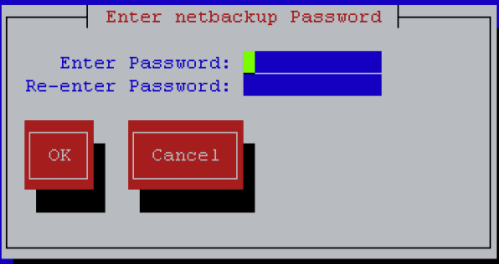
- Application server platform installation has been completed.
- NAPD has been completed to determine the network requirements for the application server, and interfaces have been configured.
- NetBackup server is available to copy, SFTP, the appropriate NetBackup client software to the application server.
- Filesystem for NetBackup client software has been created. Execute 12.11 Create LV and Filesystem for NetBackup Client Software, if the application installed on the server does not provide an alternative to creating the NetBackup logical volume.
- Config file has been created, if the version of NetBackup Client is greater than 7.5.0.0.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 106.Install/Upgrade NetBackup Client with platcfg

| Step | Procedure | Results |
|--|---|--|
| <p>1. <input type="checkbox"/></p> | <p>Application Server iLO: Login and start the integrated remote console</p> | <p>1. Log into iLO with Internet Explorer using the password provided by the application. <code>http://<management_server_iLO_IP></code></p> <p>2. Click on the Remote Console tab and open the Integrated Remote Console on the server.</p> <p>3. Click Yes if the Security Alert displays.</p> |
| <p>2. <input type="checkbox"/></p> | <p>TVOE Application Server iLO: Login</p> | <p>If the application is a guest on a TVOE host, login with application admusr credentials.</p> <p>Note: On a TVOE host, if you open the virsh console, for example, <code>\$ sudo /usr/bin/virsh console X</code> or from the virsh utility <code>virsh # console X</code> command and you get garbage characters or the output is not correct, then there is likely a stuck virsh console command already being run on the TVOE host. Exit out of the virsh console, run <code>ps -ef grep virsh</code>, and then kill the existing process <code>kill -9 <PID></code>. Then execute the <code>virsh console X</code> command. Your console session should now run as expected.</p> <p>Log into the application console using virsh and wait until you see the login prompt:</p> <pre>\$ virsh \$ virsh list --all Id Name State 13 myTPD running 20 applicationGuestName running \$ virsh console applicationGuestName [Output Removed] Starting ntdMgr: [OK] Starting atd: [OK] 'TPD Up' notification(s) already sent: [OK] upstart: Starting tpdProvd... upstart: tpdProvd started. CentOS release 6.2 (Final) Kernel 2.6.32-220.17.1.el6prere16.0.0_80.14.0.x86_64 on an x86_64 applicationGuestName login:</pre> |

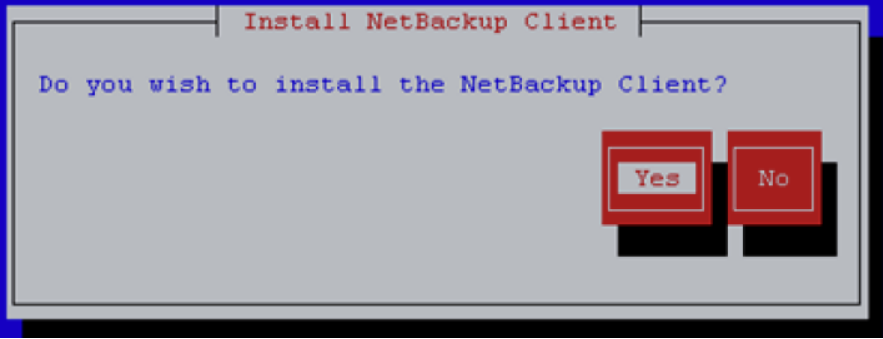
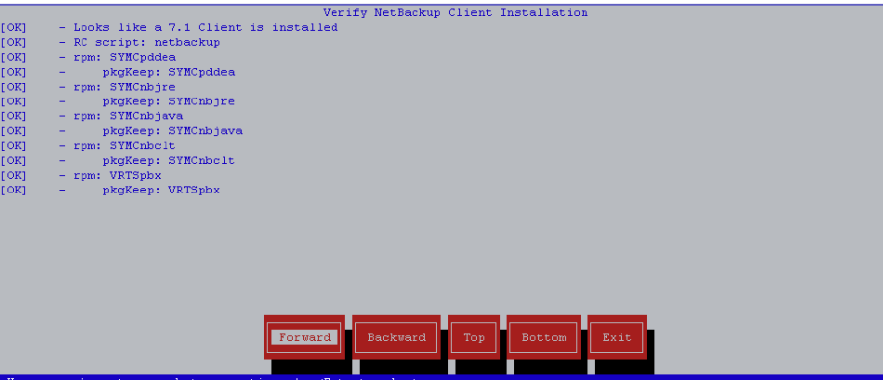
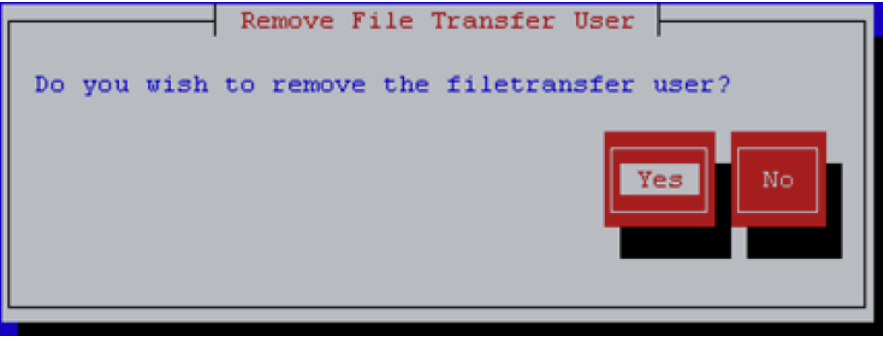
Procedure 106. Install/Upgrade NetBackup Client with platcfg

| Step | Procedure | Results |
|---|---|--|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Application Console: Configure NetBackup client on application server</p> | <p><code>\$ sudo su - platcfg</code></p> <ol style="list-style-type: none"> Navigate to NetBackup Configuration. Click Enable Push of NetBackup Client.  <p>The screenshot shows a terminal window titled "NetBackup Configuration Menu". The menu items are: "Enable Push of Netbackup Client" (highlighted in red), "Verify NetBackup Client Push", "Install NetBackup Client", "Verify NetBackup Client Installation", "Remove File Transfer User", and "Exit".</p> <ol style="list-style-type: none"> Click Yes to initialize the server and enable the Netbackup client software push.  <p>The screenshot shows a dialog box titled "Enable Push of Netbackup Client". The text inside asks: "Do you wish to initialize this server for NetBackup Client?". There are two buttons: "Yes" and "No".</p> <ol style="list-style-type: none"> Type the NetBackup password and click OK.  <p>The screenshot shows a dialog box titled "Enter netbackup Password". It has two input fields: "Enter Password:" and "Re-enter Password:". There are two buttons: "OK" and "Cancel".</p> <p>If the version of NetBackup is 7.6.0.0 or greater, follow the instructions provided by the OSDC download for the version of NetBackup that is being pushed.</p> <ol style="list-style-type: none"> Navigate to NetBackup Configuration > Verify NetBackup Client Push. Verify the list of entries indicate [OK] for the NetBackup client software environment and click Exit. |

Procedure 106. Install/Upgrade NetBackup Client with platcfg

| Step | Procedure | Results |
|-----------------|--|---|
| <p>4. □</p> | <p>NetBackup Server: Push appropriate NetBackup client software to application server</p> | <p>Notes:</p> <ul style="list-style-type: none"> • 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. These steps are required on the NetBackup server to push the NetBackup client software to the application server. • These steps assume the NetBackup server is executing in a Linux environment. • The backup server is supported by the customer, and the backup utility software provider. If this step, executed at the backup utility server, fails to execute successfully, STOP and contact Error! Bookmark not defined. for the backup and restore utility software provider being used at this site. • The NetBackup user on the client is a new user that requires the operator to change the password immediately. The operator should log into the client to change the initial password. <ol style="list-style-type: none"> 1. Log into the NetBackup server with the password provided by customer. 2. Execute the sftp_to_client NetBackup utility using the application IP address and application NetBackup user: <pre style="font-family: monospace; font-size: small;"># ./sftp_to_client 10.240.17.106 netbackup Connecting to 10.240.17.106... Password: You are required to change your password immediately (root enforced) Changing password for netbackup. (current) UNIX password: New password: Retype new password: sftp completed successfully. The root user on 10.240.17.106 must now execute the command "sh /tmp/bp.26783/client_config [-I]". The optional argument, "-I", is used to avoid modification of the client's current bp.conf file.</pre> |

Procedure 106. Install/Upgrade NetBackup Client with platcfg

| Step | Procedure | Results |
|--|--|--|
| <p>5. <input type="checkbox"/></p> | <p>Application Console: Install NetBackup client software on the application server</p> | <ol style="list-style-type: none"> Navigate to NetBackup Configuration > Install NetBackup Client. Click Yes to install the NetBackup client software.  <ol style="list-style-type: none"> Click Exit to return to the NetBackup Configuration menu. |
| <p>6. <input type="checkbox"/></p> | <p>Application Console: Verify NetBackup client software installation on the application server</p> | <ol style="list-style-type: none"> Navigate to NetBackup Configuration > Verify NetBackup Client Installation. Verify list entries indicate [OK] for NetBackup client software installation.  <ol style="list-style-type: none"> Click Exit to return to the NetBackup Configuration menu. |
| <p>7. <input type="checkbox"/></p> | <p>Application Console: Disable NetBackup client software transfer to the application server</p> | <ol style="list-style-type: none"> Navigate to NetBackup Configuration > Remove File Transfer User. Click Yes to remove the NetBackup file transfer from the application server.  |

Procedure 106. Install/Upgrade NetBackup Client with platcfg

| Step | Procedure | Results |
|--------------------------------|--|---|
| 8. <input type="checkbox"/> | Application Console: Verify the server has been added to the /usr/opensv/netbackup/bp.conf file | <pre>\$ sudo cat /usr/opensv/netbackup/bp.conf SERVER = NB76Server CLIENT_NAME = 10.240.117.134 CONNECT_OPTIONS = localhost 1 0 2</pre> |
| 9. <input type="checkbox"/> | Application Console iLO | Exit platform configuration utility (platcfg). |

12.11 Create LV and Filesystem for NetBackup Client Software

This procedure configures storage for the NetBackup client. This prevents a disk shortage in the **/usr/** filesystem.

Prerequisite: The volume group where the NetBackup logical volume resides has been previously determined. You can determine what space is available in each volume group by running the **vgs** command and looking at the **VFfree** column. Ultimately, applications should decide the volume group where the NetBackup LV should reside.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 107. Create LV and Filesystem for NetBackup Client Software

| Step | Procedure | Results |
|--------------------------------|---|--|
| 1. <input type="checkbox"/> | Server: Login | Login as the admusr user |
| 2. <input type="checkbox"/> | Server: Create a storageMgr configuration file that defines the LV to be created | <pre>\$ sudo echo "lv --mountpoint=/usr/opensv --size=5G --name=netbackup_lv --vg=\$VG" > /tmp/nb.lvm</pre> This example uses the \$VG as the volume group. Replace \$VG with the desired volume group as specified by the application group. |
| 3. <input type="checkbox"/> | Server: Create the LV and filesystem by using storageMgr | <pre>\$ sudo /usr/TKLC/plat/sbin/storageMgr /tmp/nb.lvm</pre> This creates the LV, formats it with a filesystem, and mounts it under /usr/opensv/ . For example: <pre>Called with options: /tmp/nb.lvm VG vgguests already exists. Creating lv netbackup_lv. Volume netbackup_lv will be created. Success: Volume netbackup_lv was created. Creating filesystem, this may take a while. Updating fstab for lv netbackup_lv. Configuring existing lv netbackup_lv.</pre> |

12.12 Migrate NetBackup Client to New Filesystem

This procedure migrates the installed files for NetBackup client from the **/usr/** filesystem to a filesystem dedicated to NetBackup client.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 108.Migrate NetBackup Client to New Filesystem

| Step | Results |
|--------------------------------|---|
| 1. <input type="checkbox"/> | From the server, login as the admusr user. |
| 2. <input type="checkbox"/> | Stop the NetBackup services. <pre>\$ sudo service netbackup stop</pre> <pre>\$ sudo service vxpbx_exchanged stop</pre> |
| 3. <input type="checkbox"/> | Bind mount /usr/openv to a temporary mount point. <pre>\$ sudo mkdir /tmp/openv</pre> <pre>\$ sudo mount --bind /usr/openv /tmp/openv</pre> |
| 4. <input type="checkbox"/> | Create the LV and filesystem using 12.11 Create LV and Filesystem for NetBackup Client Software. |
| 5. <input type="checkbox"/> | Move all contents of /tmp/openv to /usr/openv . <pre>\$ sudo mv /tmp/openv/* /usr/openv</pre> |
| 6. <input type="checkbox"/> | Unmount bind mount and remove mount point. <pre>\$ sudo unmount /tmp/openv</pre> <pre>\$ sudo rmdir /tmp/openv</pre> |
| 7. <input type="checkbox"/> | Start the NetBackup services. <pre>\$ sudo service vxpbx_exchanged start</pre> <pre>\$ sudo service netbackup start</pre> |

12.13 Create NetBackup Client Config File

This procedure copies NetBackup Client config file into the appropriate location on the TPD based application server. This config file allows a customer to install previously unsupported versions of NetBackup Client by providing necessary information to TPD.

The contents of the config file are provided by **Error! Bookmark not defined.** Contact **Error! Bookmark not defined.** you are attempting to install an unsupported version of NetBackup Client.

Prerequisites:

- The TPD-NetBackup RPM has been installed on the server.
- The contents of the NetBackup Client config file are known.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 109. Create NetBackup Client Config File

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | Server: Create NetBackup client config file | <p>Create the NetBackup client config file on the server using the contents that were previously determined. The config file should be placed in the /usr/TKLC/plat/etc/netbackup/profiles directory and should follow the following naming NB\$ver.conf conventions. Where \$ver is the client version number with the periods removed. For the 7.5 client the value of \$ver would be 75 and the full path to the file would be /usr/TKLC/plat/etc/netbackup/profiles/NB75.conf.</p> <p>Note: The config files must start with NB and must have a suffix of .conf. The server is now capable of installing the corresponding NetBackup client.</p> <p>The server is now capable of installing the corresponding NetBackup client.</p> |
| 2. <input type="checkbox"/> | Server: Create NetBackup client config file script | <p>Create the NetBackup client config script file on the server using the contents that were previously determined. The config script file should be placed in the /usr/TKLC/plat/etc/netbackup/scripts directory. The name of the NetBackup client config script file should be determined from the contents of the NetBackup client config file. As an example for the NetBackup 7.5 client the following is applicable:</p> <p>NetBackup client config: /usr/TKLC/plat/etc/netbackup/profiles/NB75.conf</p> <p>NetBackup client config script: /usr/TKLC/plat/etc/netbackup/scripts/NB75</p> |

13. TVOE Host Procedures

13.1 Enable Virtual Guest Watchdogs as Appropriate for the Application

This procedure describes how to use the PMAC application on the management server to enable the virtual guest watchdog on VM guests after upgrading a TVOE VM host to a version that adds watchdog support (TVOE version 2.0.0_80.11.0 or later).

Prerequisite: One or more installations of TVOE have been upgraded to TVOE version 2.0.0_80.11.0 or later.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 110. Enable Virtual Guest Watchdogs as Appropriate for the Application

| Step | Results |
|--------------------------------|--|
| 1. <input type="checkbox"/> | On the PMAC managing each newly upgraded TVOE server, navigate to Main Menu > VM Management on the PMAC GUI. |
| 2. <input type="checkbox"/> | From the VM Entities list, locate the host just upgraded and click + to expand the list of VM guests. |

Procedure 110.Enable Virtual Guest Watchdogs as Appropriate for the Application

| Step | Results |
|--------------------------------|---|
| 3. <input type="checkbox"/> | <p>Select each VM guest on the TVOE host where virtual watchdog support is needed:</p> <ol style="list-style-type: none"> 1. Shut down the VM guest by setting its power state to Shutdown and clicking the adjacent Change to. Wait for the shutdown to complete as indicated by the Current Power State field of the GUI. 2. Click Edit to enter edit mode for this VM Guest. 3. Mark the Enable Virtual Watchdog checkbox. 4. Click Save and wait for the edit operation to finish. 5. Start the VM guest by setting the power state to On and clicking Change to. 6. When the VM Guest's power state indication shows Running, proceed to the next VM guest on this host. |

13.2 Configure TVOE NetBackup Client

This procedure sets up and installs the NetBackup client on a TVOE host.

Note: Once the NetBackup Client is installed on TVOE, the NetBackup Master should be configured to back up the following file from the TVOE host.

`/var/TKLC/bkp/*.iso`

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 111.Configure TVOE NetBackup Client

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | TVOE Server: Login | Login as the admusr user. |
| 2. <input type="checkbox"/> | TVOE Server: Open firewall ports for NetBackup | <pre>\$ sudo ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt /usr/TKLC/plat/etc/iptables/ \$ sudo ln -s /usr/TKLC/plat/share/netbackup/60netbackup.ipt /usr/TKLC/plat/etc/ip6tables/ \$ sudo /usr/TKLC/plat/bin/iptablesAdm reconfig</pre> |
| 3. <input type="checkbox"/> | TVOE Server: Enable platcfg to show the NetBackup menu items | <pre>\$ sudo platcfgadm --show NBConfig \$ sudo platcfgadm --show NBInit \$ sudo platcfgadm --show NBDeInit \$ sudo platcfgadm --show NBInstall \$ sudo platcfgadm --show NBVerifyEnv \$ sudo platcfgadm --show NBVerify</pre> |
| 4. <input type="checkbox"/> | TVOE Server: Create LV and filesystem for NetBackup client software | Using the vgguests volume group, execute 12.11 Create LV and Filesystem for NetBackup Client Software to create an LV and filesystem for the NetBackup client software. |

Procedure 111. Configure TVOE NetBackup Client

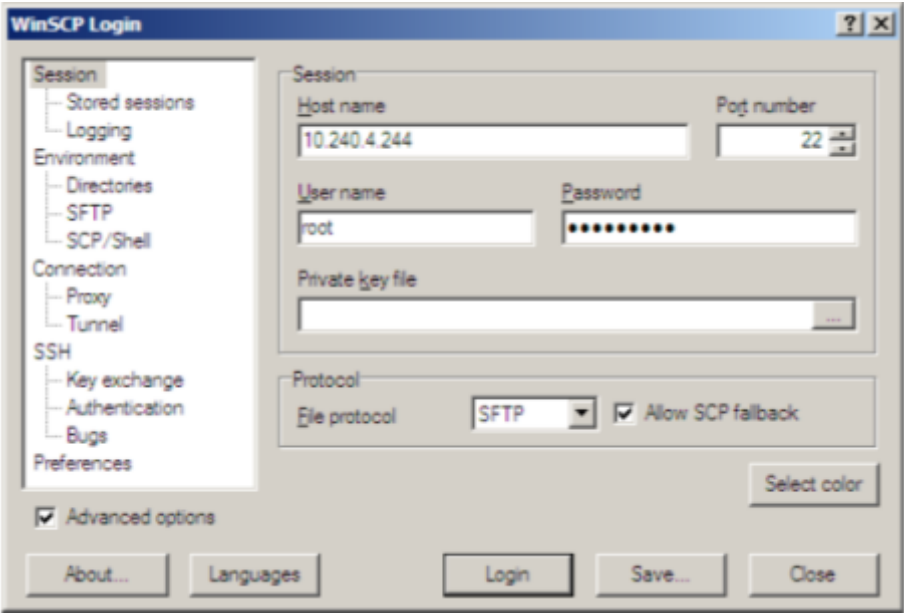
| Step | Procedure | Results |
|--------------------------------|---|---|
| 5. <input type="checkbox"/> | TVOE Server: Install NetBackup client software | Execute 12.5 Install the NetBackup Client . Note: Skip any steps relating to copying NetBackup notify scripts to /usr/openv/netbackup/bin. The TVOE NetBackup notify scripts are taken care of in the next step. |
| 6. <input type="checkbox"/> | TVOE Server: Create soft links for TVOE specific NetBackup notify scripts | <pre>\$ sudo ln -s /usr/TKLC/plat/sbin/bpstart_notify /usr/openv/netbackup/bin/bpstart_notify \$ sudo ln -s /usr/TKLC/plat/sbin/bpend_notify /usr/openv/netbackup/bin/bpend_notify</pre> |

Appendix A. Using WinSCP

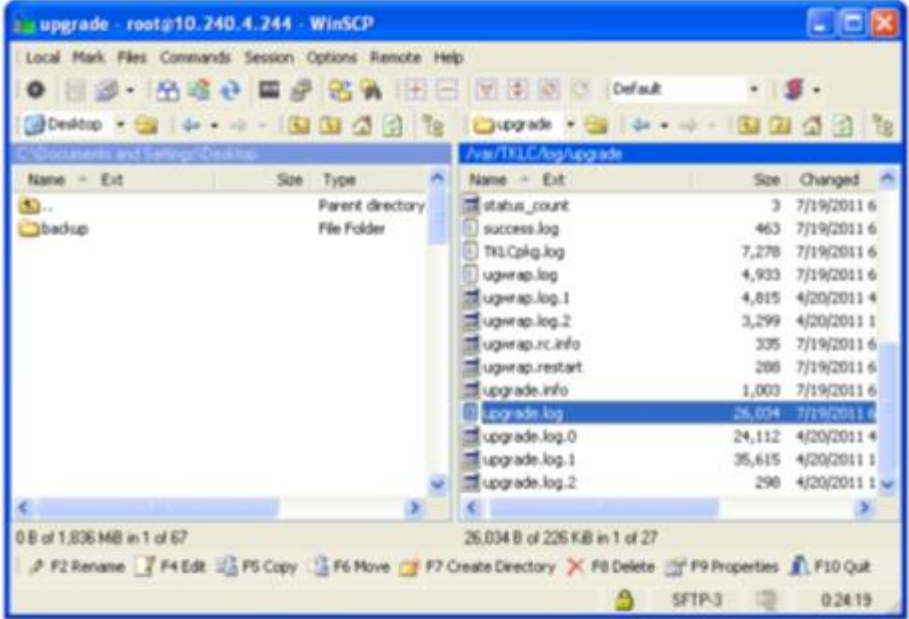
This procedure demonstrates how to copy a file from the management server to your PC desktop.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 112. Copy a File from the Management Server to the PC Desktop

| Step | Procedure | Results |
|--------------------------------|----------------------------------|--|
| 1. <input type="checkbox"/> | Download the WinSCP application | http://winscp.net/eng/download.php |
| 2. <input type="checkbox"/> | Connect to the management server | <p>After starting this application, navigate to Session and enter: <management_server_IP> into the Host name field, root into the User name field, and <root_password> into the Password field. Click Login.</p>  |

Procedure 112. Copy a File from the Management Server to the PC Desktop

| Step | Procedure | Results |
|---|--|--|
| <p>3.</p> <p><input type="checkbox"/></p> | <p>Copy the target file from the management server</p> | <p>On the left is your own desktop filesystem. Navigate within it to Desktop directory. On the right side is the management server file system. Within it, navigate into the location of the file you would like to copy to your desktop. Highlight the file in the management server file system by pressing the insert key, and then press F5 to copy the file.</p>  <p>The screenshot shows the WinSCP interface with two panes. The left pane shows the local PC's Desktop directory with a 'backup' folder. The right pane shows the remote management server's file system, specifically the path 'Avi/TKL/Log/Upgrade'. A file named 'log.adn.log' is selected and highlighted in blue. The status bar at the bottom indicates 'SFTP-3' and '0.2419'.</p> |
| <p>4.</p> <p><input type="checkbox"/></p> | <p>Close the WinSCP application</p> | <p>Press F10 and click OK to confirm terminating the session.</p> |

Appendix B. Install P2000 MSA USB Driver

The P2000 USB driver allows Microsoft Windows to recognize the USB port on HP StorageWorks P2000 G3 MSA Controllers. This appendix describes how to install the driver on your laptop.

Prerequisite: 9.8 Add ISO Images to the PMAC Image Repository has been completed using the HP MISC firmware ISO image.


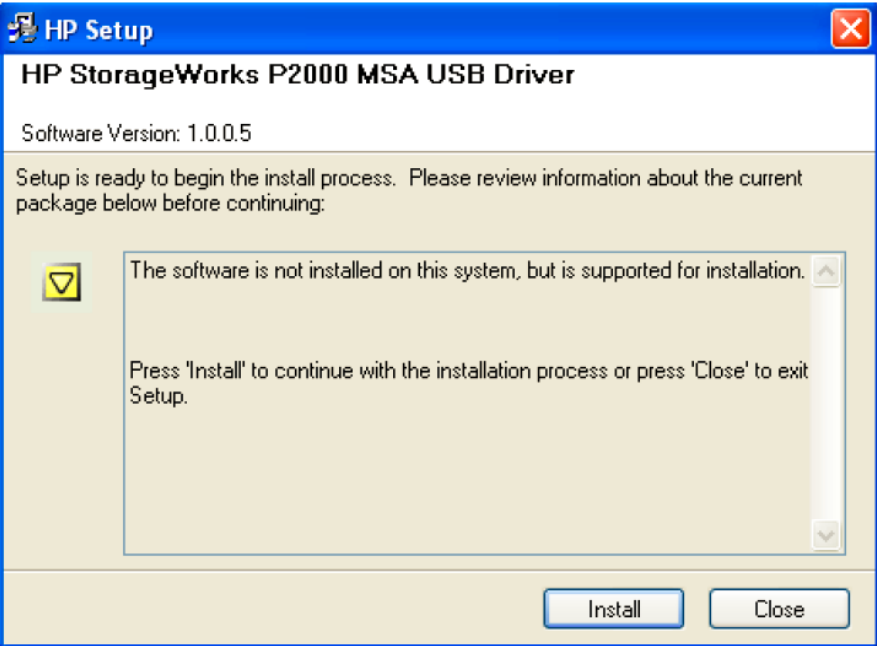
Note: If you are unable to detect the P2000 array after installing the USB driver, power cycle the P2000 array once.

Needed Material

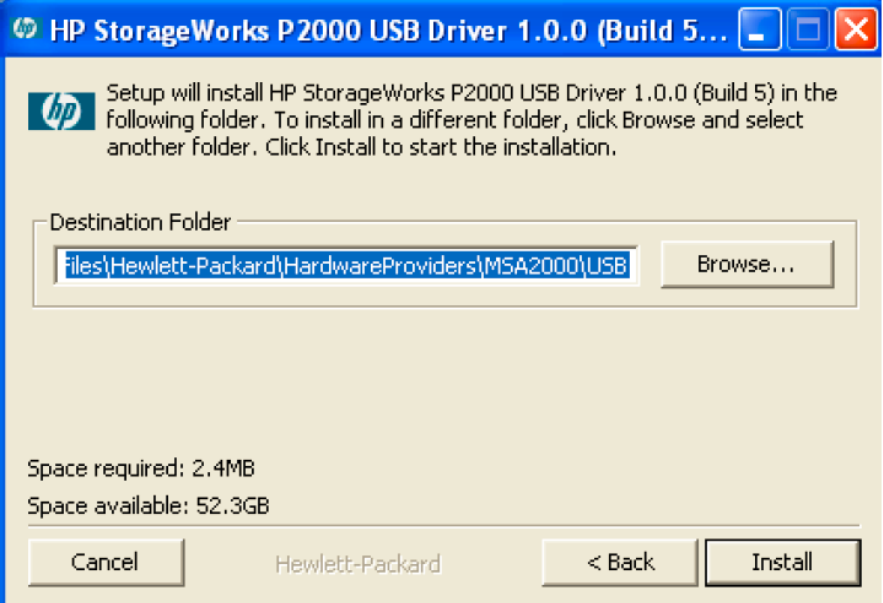
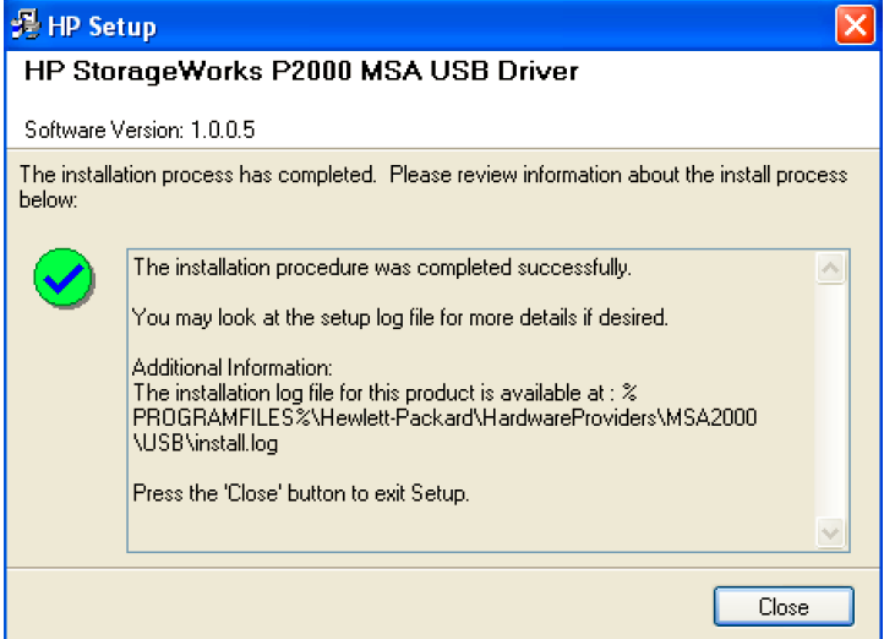
- HP MISC firmware ISO image
- [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 113. Install P2000 MSA USB Driver

| Step | Procedure | Results |
|--|---|--|
| <p>1. <input type="checkbox"/></p> | <p>Management Server: Obtain the USB driver executable</p> | <p>Copy the following from the management server to your PC using an SCP client.</p> <pre data-bbox="548 373 1182 426">/usr/TKLC/smac/html/TPD/HPFW--872-2488-XXX--HPFW/files/<USB_Driver>.exe</pre> <p>Windows users need to refer to Appendix A Using WinSCP to copy the zip file to you PC.</p> <p>Refer to [3] HP Solutions Firmware Upgrade Pack, Software Centric Release Notes to select the correct file to copy.</p> |
| <p>2. <input type="checkbox"/></p> | <p>Microsoft Windows Laptop: Initiate the setup wizard</p> | <p>Click the USB Driver executable on your laptop. If a security window displays asking whether to run the executable, click Run.</p>  <p>The screenshot shows a dialog box titled "HP Package Setup" with a close button (X) in the top right corner. The main text says: "HP Setup is ready to install the contents of this package. Press 'Install' to run the installation program or press 'Extract...' to only extract the files." Below this, there is a section for "HP StorageWorks P2000 MSA USB Driver" with "Version: 1.0.0.5". A descriptive paragraph follows: "The P2000 USB Driver allows Microsoft Windows to recognize the USB Port on HP StorageWorks P2000 G3 MSA Controllers." On the right side, there are three buttons: "Install", "Extract...", and "Close".</p> |
| <p>3. <input type="checkbox"/></p> | <p>Microsoft Windows Laptop: Agree to installation</p> | <p>Click Install.</p>  <p>The screenshot shows a dialog box titled "HP Setup" with a close button (X) in the top right corner. The main text says: "HP StorageWorks P2000 MSA USB Driver" and "Software Version: 1.0.0.5". Below that, it says: "Setup is ready to begin the install process. Please review information about the current package below before continuing:". There is a checked checkbox with a yellow triangle icon next to a text box containing: "The software is not installed on this system, but is supported for installation." Below this text box, it says: "Press 'Install' to continue with the installation process or press 'Close' to exit Setup." At the bottom, there are two buttons: "Install" and "Close".</p> <p>In the next window, click I agree to proceed with the installation.</p> |

Procedure 113. Install P2000 MSA USB Driver

| Step | Procedure | Results |
|------------------------------------|---|---|
| <p>4. <input type="checkbox"/></p> | <p>Microsoft Windows Laptop: Select installation directory</p> | <p>Click Browse to select the folder where to install.</p>  <p>Click Install.</p> |
| <p>5. <input type="checkbox"/></p> | <p>Microsoft Windows Laptop: Verify installation</p> | <p>Click Close.</p>  |



Appendix C. Determine which Onboard Administrator is Active

This procedure determines which onboard administrator is active in an enclosure with two OAs.

Prerequisite: 7.2 Configure Initial OA Settings Using the Configuration Wizard

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 114. Determine which Onboard Administrator is Active

| Step | Procedure | Results |
|---|--|---|
| <p>1.</p> <p><input type="checkbox"/></p> | <p>OA GUI: Determine which OA is active</p> | <p>Open a web browser and navigate to the IP address of one of the administrators.</p> <p>http://winscp.net/eng/download.php</p> <p>If you see the following screen, you have navigated to a GUI of the standby OA as indicated by the red warning. In such a case, navigate to the other Onboard Administrator IP address.</p>  <p>If you navigate to the active Onboard Administrator GUI, the enclosure overview table is available in the left part of the login screen.</p>  |

Appendix D. PMAC Features Configuration

Appendix D.1 Overview

PMAC configuration manages identified software features. Features implemented by PMAC may be defined as editable in profiles used during PMAC Initialization. This is typically decided and specified in profiles by developers. When a feature is defined as editable, it may be managed by authorized users using the PMAC GUI or CLI. Features may be enabled or disabled, and their associated role may be changed (used for features that expose or configure services on a network interface basis).

Appendix D.2 Enabling Features

Enabling features may affect available APIs (that is, fail the requests), configure services (for example, configure TFTP), or configure the host firewall. From the CLI, you may administratively disable a feature to block actions temporarily. This is useful for NetBackup to prevent actions affecting the backup images, or netConfig to prevent conflicts with TFTP services. Administratively disabled services are either enabled manually or enabled when PMAC is restarted.

Appendix D.3 Editing Roles

Feature roles are used to associate a feature with a particular set of interfaces. This is used to manage the host firewall or configure services. New roles may be defined and applied to dedicated interfaces. For instance, NetBackup is often provided a unique role. You should understand the network and product before changing roles. The **control**, **management**, and **NetBackup** roles are currently used by products. PMAC was designed to be flexible, so you are able to create roles and map them to interfaces as desired (that is, expanding a system may need to add new non-contiguous networks for control or management).

Appendix D.4 Features

Features are declared as user editable by profiles. The current PMAC 6.6 TVOE profile exposes the following features:

- **DEVICE.NETWORK.NETBOOT** is used to allow netConfig to initialize Cisco 3020 switches that use TFTP. It is typically enabled on the "management" role.
- **DEVICE.NTP** allows devices to use PMAC as an NTP server. By default, the port is blocked by the firewall.
- **PMAC.MANAGED** allows remote systems to access the SNMP service on PMAC.
- **PMAC.REMOTE.BACKUP** is another optional feature.
- **PMAC.NETBACKUP** is an optional feature that should be enabled if NetBackup is used.
- **PMAC.IPV6.NOAUTOCONFIG** is an optional feature that disables auto-configuration of IPv6 on PMAC interfaces.

To add features as editable, they must be declared in the profile during PMAC Initialization. If PMAC is in service, you must use the CLI to reset and re-initialize PMAC. To prevent profile changes from being lost during upgrade, you should avoid modifying profiles delivered with PMAC. Best practice is to copy the profile and edit this version.

Appendix D.5 GUI Usage

From the PMAC GUI, navigate to **Administration > PMAC Configuration > Feature Configuration**.

Click **Apply** to reconfigure the platform.

Appendix D.6 CLI Usage

The `pmacadm` CLI allows features to be modified also. This is the only interface to disable a feature administratively. The options on the `pmacadm` command map to integers for the enable/disable states (see `man pmacadm`).

For example, to disable the `DEVICE.NETWORK.NETBOOT` feature:

```
$ sudo /usr/TKLC/smac/bin/pmacadm editFeature --featureName=DEVICE.NETWORK.NETBOOT --enable=0
$ sudo /usr/TKLC/smac/bin/pmacadm resetFeatures
```

Appendix E. Access and Exit a Server Console Remotely Using iLO

This procedure accesses a server console remotely.

Steps within this procedure may refer to variable data indicated by text within `<>`. Refer to this table for the proper value to insert depending on your system type.

| Variable | Value |
|--------------------------------------|--|
| <code><iLO_admin_user></code> | Privileged username for HP iLO access |
| <code><iLOM_admin_user></code> | Privileged username for Oracle RMS ILOM access |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Appendix E.1 Access a Server Console Remotely

Procedure 115. Access a Remote Server Console

| Step | Procedure | Results |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Access the iLO/iLOM GUI | Using a laptop or desktop computer connected to the customer network, navigate with Internet Explorer to the IP address of the iLO/iLOM on the management server. Click Continue to this website (not recommended) if prompted. Log into the iLO as the <code><iLO_admin_user></code> . |
| 2. <input type="checkbox"/> | If the iLO is an iLO2: Configure hot keys | The iLO GUI indicates the iLO version as iLO 2 ("Integrated Lights-Out 2"), iLO 3, iLO 4, etc. If this is an iLO 2, perform the following Hot Key configuration: 1. Click the Remote Console tab. 2. Click the Settings menu item and the Hot Keys sub-tab. 3. In the row starting with Ctrl-T , change the first dropdown to L_CTRL and the second dropdown to] (right bracket). The rest of the dropdowns in the row should be NONE. 4. In the row starting with Ctrl-v , change the first drop down to L_CTRL , the second dropdown to R_Shift , and the third dropdown to - . The rest of the dropdowns in the row should be NONE. 5. Click Save Hot Keys . As a result, pressing Ctrl-T rather than Ctrl-] exits the console of a TVOE guest and returns to the console of the TVOE host. Pressing Ctrl-v disconnects the switch console session. |

Procedure 115. Access a Remote Server Console

| | | |
|--|---------------------------------------|--|
| <p>3. <input type="checkbox"/></p> | <p>Open the remote console window</p> | <p>For HP servers: Click the Remote Console tab and select Remote Console to open the remote console in a new window. If prompted, click Continue on the Security Warning screen.</p> <p>For Oracle rack mount servers: Click Launch beside the Remote Console in the Actions frame. Click Continue if a Security Warning screen displays. Click Run.</p> |
| <p>4. <input type="checkbox"/></p> | <p>Log into the console</p> | <p>In the Remote Console window, log into the console as the admusr.</p> <pre> Login as: admusr Password: Last login: Fri Oct 6 17:52:28 2017 [admusr@tvo ~]\$ </pre> |

Appendix E.2 Exit a Guest Console Session on an iLO

This procedure exits a guest console session on an iLO.

Enter the control sequence for the iLO version.

If the main iLO GUI window indicates that this is an iLO2 (Integrated Lights-Out 2), press **Ctrl-T**. Otherwise, press **Ctrl-]**. This step corresponds to the configuration of iLO 2 Hot Keys performed in Appendix E.1, step 2.



Appendix F. Attach an ISO Image to a Server Using iLO or iLOM

Appendix F.1 Attach an ISO Image to an HP Server Using iLO


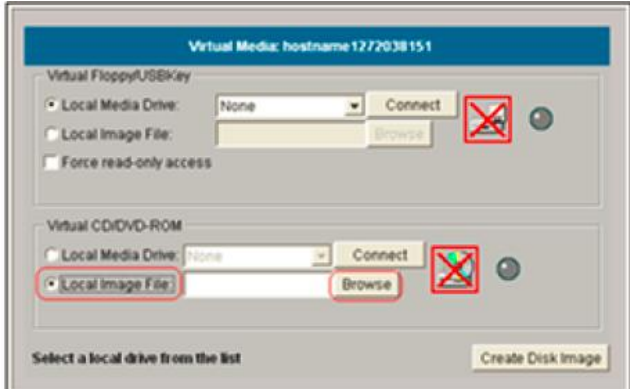
This procedure attaches an ISO image to an HP server.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

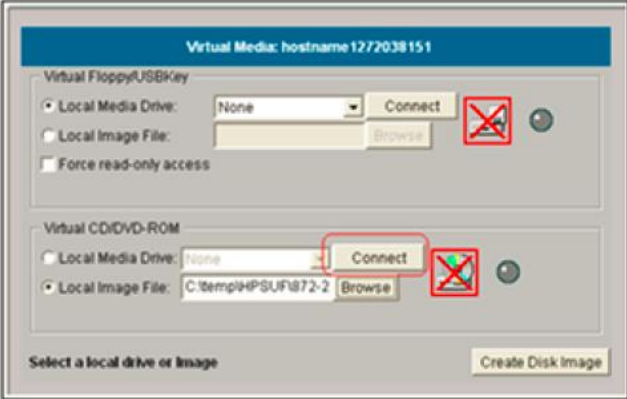

Procedure 116. Attach an ISO Image to an HP Server Using iLO

| Step | Procedure | Results |
|--|---|--|
| <p>5. <input type="checkbox"/></p> | <p>Local Workstation: Access the iLO Web GUI and login</p> | <p>Log into the ProLiant Server using Internet Explorer: <a href="https://<iilo_IP>/">https://<iilo_IP>/ Username: <iilo_admin_user> Password: <iilo_admin_password></p>  |
| <p>6. <input type="checkbox"/></p> | <p>Local Workstation: Determine iLO version</p> | <p>If the iLO GUI indicates Integrated Lights-Out 2, then continue to the next step. If the iLO GUI indicates Integrated Lights-Out 3 or Integrated Lights-Out 4, then continue to step 12. .</p> |
| <p>7. <input type="checkbox"/></p> | <p>iLO2 Web GUI: Access virtual media</p> | <p>Navigate to Summary -> Virtual Media.</p>  |

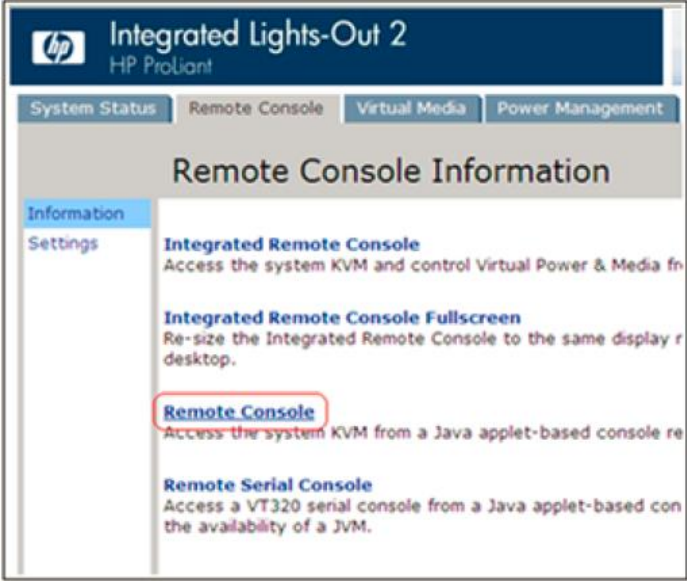
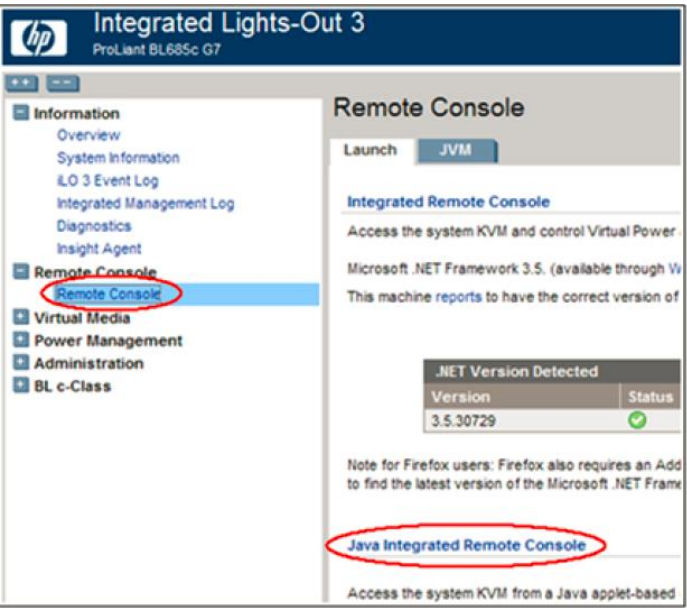
Procedure 116. Attach an ISO Image to an HP Server Using iLO

| Step | Procedure | Results |
|--|---|--|
| <p>8. <input type="checkbox"/></p> | <p>iLO2 Web GUI: Open Virtual Media Applet</p> | <p>Click Virtual Media Applet.</p>  <p>Click Yes to acknowledge the security warning. If other screens display, acknowledge them as well.</p> |
| <p>9. <input type="checkbox"/></p> | <p>iLO 2 VM Applet: Select ISO file</p> | <p>In the Virtual CD/DVD-ROM panel, select the Local Image File option and click Browse. Navigate to the ISO image file specified by the procedure that referenced this appendix.</p>  <p>Select the ISO image file and click Open.</p> |

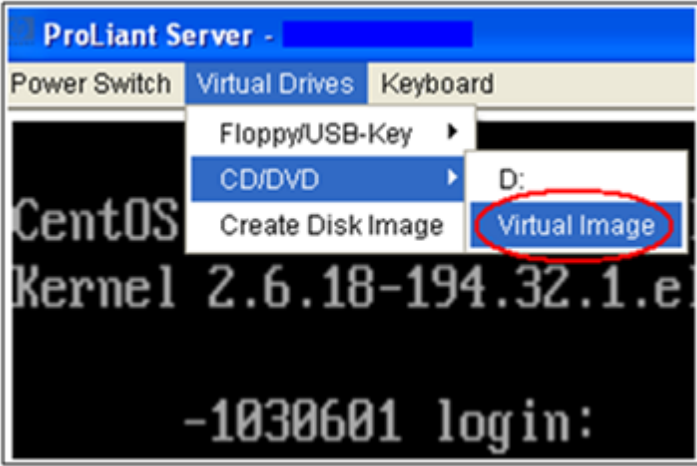
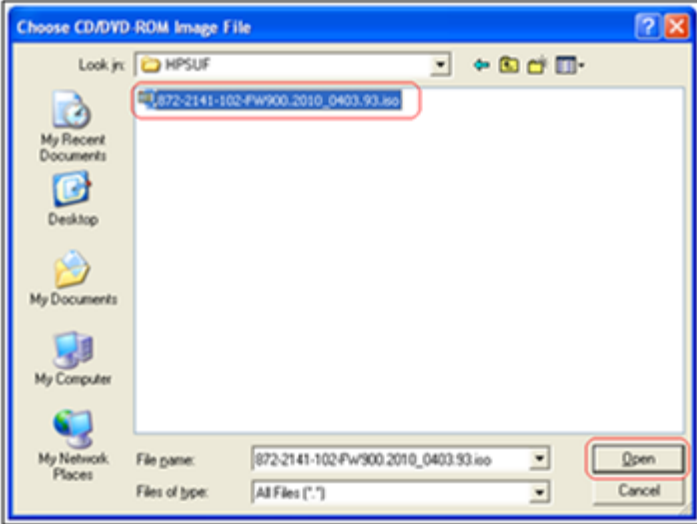

Procedure 116. Attach an ISO Image to an HP Server Using iLO

| Step | Procedure | Results |
|------------------|--|---|
| <p>10. □</p> | <p>iLO 2 VM Applet: Create a virtual drive connection</p> | <p>Click Connect to create a virtual DVD-ROM connection to the ISO image file.</p>  <p>The light icon turns green.</p>  <p>DO NOT close the applet and return to the browser window with the iLO Web GUI.</p> |

Procedure 116. Attach an ISO Image to an HP Server Using iLO

| Step | Procedure | Results |
|------------------|---|---|
| <p>11. □</p> | <p>iLO2 Web GUI: Open Remote Console applet</p> | <p>Click on the Remote Console tab. Click Remote Console.</p>  <p>Click Yes to acknowledge the security warning. If other screens display, acknowledge them as well. Return to procedure that referenced this appendix.</p> |
| <p>12. □</p> | <p>iLO3/iLO4 Web GUI: Open Remote Console applet</p> | <p>From the left side menu, click Remote Console. Click Java Integrated Remote Console.</p>  <p>Click Yes to acknowledge the security warning.</p> |

Procedure 116. Attach an ISO Image to an HP Server Using iLO


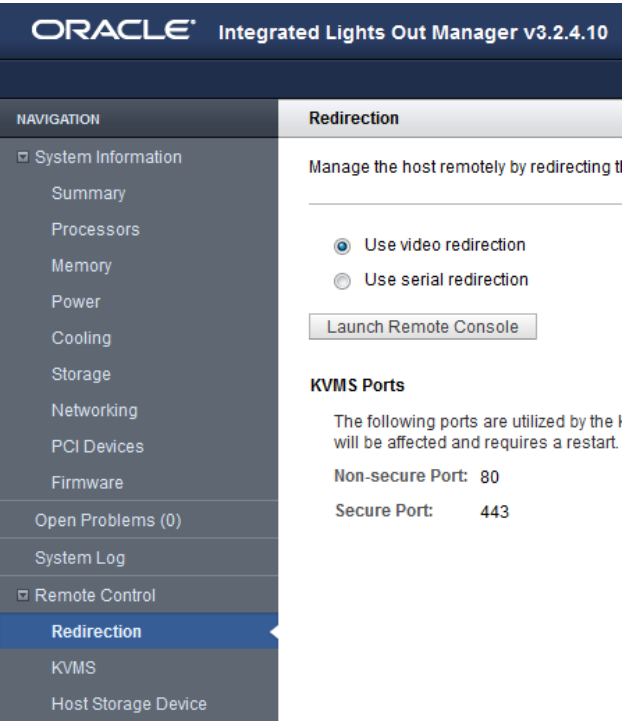
| Step | Procedure | Results |
|------------------|--|---|
| <p>13. □</p> | <p>iLO3/iLO4 Web GUI: Open virtual image</p> | <p>Navigate to Virtual Drives -> CD/DVD -> Virtual Image.</p>  <p>Navigate to the location of the ISO image file specified by the procedure referenced in this appendix.</p>  <p>Select the desired file and click Open.</p> |
| <p>14. □</p> | <p>iLO3/iLO4 Web GUI: Verify virtual image connection</p> | <p>At the bottom of the remote console window, there should now be a green highlighted drive icon and Virtual M written next to it.</p>  <p>Return to procedure that referenced this appendix.</p> |

Appendix F.2 Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

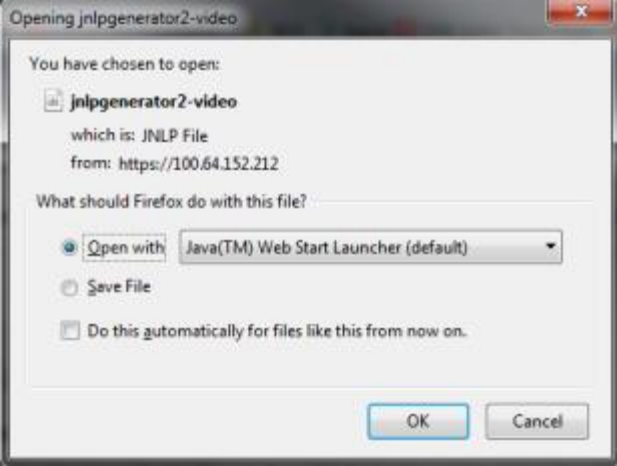

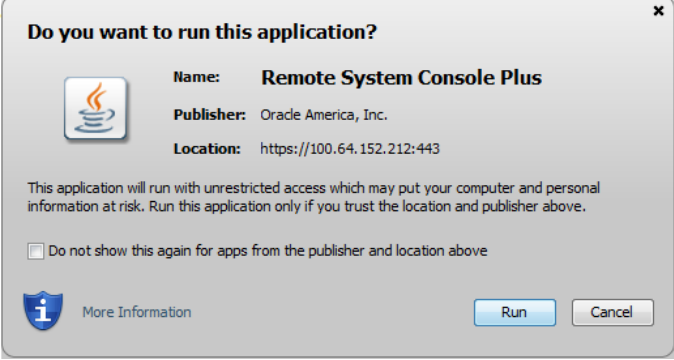
This procedure attaches an ISO image to an Oracle rack mount server.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

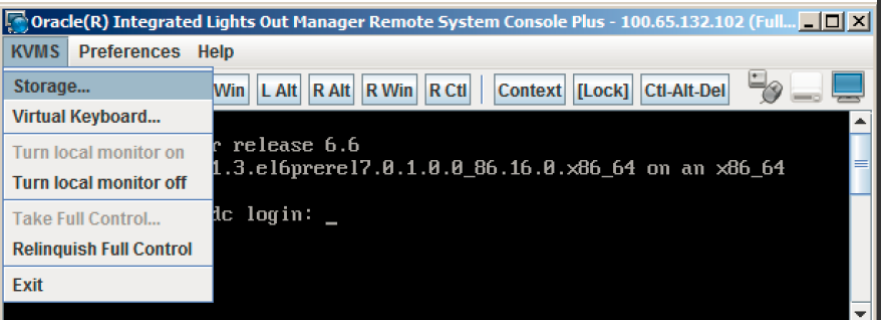
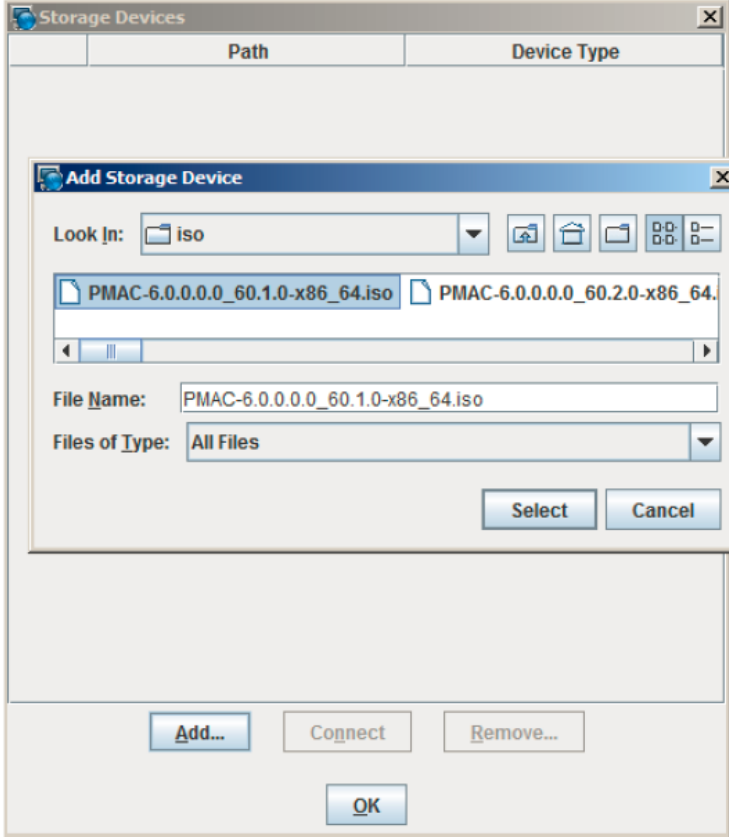
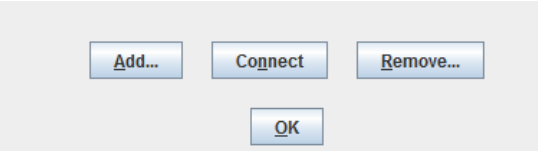
Procedure 117. Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

| Step | Procedure | Results |
|-----------------|--|---|
| <p>1. □</p> | <p>Local Workstation: Access the ILOM Web GUI and login</p> | <p>From: <a href="https://<i lom_IP>/">https://<i lom_IP>/ Log into the Oracle rack mount server ILOM.</p>  |
| <p>2. □</p> | <p>ILOM Web GUI: Access the remote console</p> | <p>Navigate to Remote Control -> Redirection. Click Launch Remote Console.</p>  |

Procedure 117. Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

| Step | Procedure | Results |
|-----------------|---|---|
| <p>3. □</p> | <p>ILOM Web GUI: Access the remote console</p> | <p>Click OK and open with Java Web Start Launcher.</p>  <p>Select Continue and Run for any security warning prompts.</p>   |

Procedure 117. Attach an ISO Image to an Oracle Rack Mount Server Using iLOM

| Step | Procedure | Results |
|---|--|---|
| <p>4.</p> <p><input type="checkbox"/></p> | <p>ILOM Remote Console: Mount the ISO from the remote console</p> | <p>Navigate to KVMS -> Storage.</p>  <p>Click Add and browse to the ISO located on the local machine.</p>  <p>Click Select.</p> <p>Once the ISO image is selected, click Connect.</p>  |

Appendix G. Upgrade Cisco 4948 PROM

This procedure upgrade the Cisco 4948 PROM.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 118.Upgrade Cisco 4948 PROM

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Virtual PMAC/ Management Server: Verify the PROM image is on the system | <p>If the appropriate image does not exist, copy the image to the server. Determine if the PROM image for the 4948/4948E/4948E-F is on the system.</p> <p>For a PMAC system:</p> <pre>\$ ls /var/TKLC/smac/image/<PROM_image_file></pre> <p>For a NON-PMAC system:</p> <pre>\$ ls /var/lib/tftpboot/<PROM_image_file></pre> <p>If the file exists, skip the remainder of this step and continue with the next step. If the file does not exist, copy the file from the firmware media and ensure the file is specified by the Release Notes of [2] HP Solutions Firmware Upgrade Pack.</p> |
| 2. <input type="checkbox"/> | Virtual PMAC/ Management Server: Attach to switch console | <p>If upgrading the firmware on switch1A, connect serially to the switch by issuing the following command as admusr on the server:</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1A_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter `^Ec?' for help]</pre> <p>Press Enter.</p> <p>If the switch is not already in enable mode (switch# prompt), then issue the enable command; otherwise, continue with the next step.</p> <pre>Switch> enable</pre> <p>If upgrading the firmware on switch1B, connect serially to switch1B by issuing the following command as admusr on the PMAC server:</p> <pre>\$ sudo /usr/bin/console -M <management_server_mgmt_ip_address> -l platcfg switch1B_console Enter platcfg@pmac5000101's password: <platcfg_password> [Enter `^Ec?' for help]</pre> <p>Press Enter.</p> <p>If the switch is not already in enable mode (switch# prompt), then issue the enable command; otherwise, continue with the next step.</p> <pre>Switch> enable</pre> |

Procedure 118.Upgrade Cisco 4948 PROM

| Step | Procedure | Results |
|-----------------|---|---|
| <p>3. □</p> | <p>Virtual PMAC/ Management Server (Switch Console Session): Configure ports on the 4948/4948E/ 4948E-F switch</p> | <p>To ensure connectivity, ping the management server's management vlan IP <pmac_mgmt_ip_address> address from the switch.</p> <pre>Switch# conf t</pre> <p>If upgrading the firmware on switch1A, use these commands:</p> <pre>Switch(config)# vlan <switch_mgmtVLAN_id> Switch(config-vlan)# int vlan <switch_mgmtVLAN_id> Switch(config-if)# ip address <switch1A_mgmtVLAN_ip_address> <netmask> Switch(config-if)# no shut Switch(config-if)# int gil/40</pre> <p>If upgrading the firmware on switch1B, use these commands:</p> <pre>Switch(config)# vlan <switch_mgmtVLAN_id> Switch(config-vlan)# int vlan <switch_mgmtVLAN_id> Switch(config-if)# ip address <switch1B_mgmtVLAN_ip_address> <netmask> Switch(config-if)# no shut Switch(config-if)# int gil/40</pre> <p>If the model is 4948, execute these commands:</p> <pre>Switch(config-if)# switchport trunk encap dot1q Switch(config-if)# switchport mode trunk Switch(config-if)# spanning-tree portfast trunk Switch(config-if)# end Switch# write memory</pre> <p>If the model is 4948E or 4948E-F, execute these commands:</p> <pre>Switch(config-if)# switchport mode trunk Switch(config-if)# spanning-tree portfast trunk Switch(config-if)# end Switch# write memory</pre> <p>Issue ping command:</p> <p>Note: The IP address <pmac_mgmt_ip_address> is in the reference table at the beginning of the Cisco 4948 configuration procedure that referenced this procedure.</p> <pre>Switch# ping <pmac_mgmtVLAN_ip_address> Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to <pmac_mgmt_ip_address>, timeout is 2 seconds: !!!! Success rate is 100 percent (5/5), round trip min/avg/max = 1/1/4 ms</pre> <p>If ping is not successful, make sure the procedure was completed correctly by repeating all steps up to this point. If after repeating those steps, ping is still unsuccessful, then contact Error! Bookmark not defined.</p> |

Procedure 118.Upgrade Cisco 4948 PROM

| Step | Procedure | Results |
|--------------------------------|--|--|
| 4. <input type="checkbox"/> | Virtual PMAC/ Management Server (Switch Console Session): Upgrade PROM | <pre>Switch# copy tftp: bootflash: Address or name of remote host []? <pmac_mgmt_ip_address> Source filename []? <PROM_image_file> Destination filename [<PROM_image_file>]? [Enter] Accessing tftp://<pmac_mgmt_ip_address>/<PROM_image_file>... Loading <PROM_image_file> from <pmac_mgmt_ip_address> (via Vlan2): !!!!! [OK- 45606 bytes] 45606 bytes copied in 3.240 secs (140759 bytes/sec)</pre> |
| 5. <input type="checkbox"/> | Virtual PMAC/ Management Server (Switch Console Session): Reload switch | <pre>Switch# reload System configuration has been modified. Save? [yes/no]: no Proceed with reload? [confirm] [Enter] === Boot messages removed === Type Control-C when Type control-C to prevent autobooting message displays.</pre> |
| 6. <input type="checkbox"/> | Virtual PMAC/ Management Server (Switch Console Session): Upgrade PROM | <pre>rommon 1 > boot bootflash:<PROM_image_file> === PROM upgrade messages removed === System will reset itself and reboot within few seconds....</pre> |
| 7. <input type="checkbox"/> | Virtual PMAC/ Management Server (Switch Console Session): Verify upgrade | <p>The switch reboots when the firmware upgrade completes. Allow it to boot. Wait for the following line to be printed:</p> <pre>Press RETURN to get started! Would you like to terminate autoinstall? [yes]: [Enter] Switch> show version include ROM ROM: 12.2(31r)SGA1 System returned to ROM by reload</pre> <p>Review the output and look for the ROM version. Verify the version is the desired new version.</p> <p>If the switch does not boot properly, or has the wrong ROM version, contact Error! Bookmark not defined.</p> |
| 8. <input type="checkbox"/> | Virtual PMAC/ Management Server: Reset switch to factory defaults | <p>Connect serially to the switch as outlined in step 4. , and reload by performing the following commands:</p> <pre>Switch# write erase Switch# reload</pre> <p>Wait until the switch reloads, then exit from console, enter Ctrl-e + c + . and you are returned to the server prompt.</p> <p>Note: There may be messages from the switch, if asked to confirm, press Enter. If asked yes or no, type No and press Enter.</p> |

Appendix H. Operational Dependencies on Platform Account Passwords

This appendix describes the operational dependencies on platform account passwords to provide guidance in cases when the customer insists on modifying a default password. Note that changing passwords should be attempted only on systems that are fully configured and stable. Modifying passwords during system installation is strongly discouraged.

Before modifying the passwords stored on PMAC, perform a backup of PMAC databases in case you need to return to default passwords. To accomplish this, execute steps 6. through 8. in 9.5 Configure PMAC Application. To restore the passwords stored in the backup file, you can refer to steps 4 through 9 (inclusive), in Procedure 1 of the *PMAC Disaster Recovery*, latest release.

Appendix H.1 PMAC Credentials for Communication with Other System Components

This section covers the credentials the PMAC uses to communicate with services on itself or on external servers and the dependencies users must be aware of to keep PMAC fully functional. Only the credentials the PMAC considers user accessible are listed here.

Note: Users in the PMAC database are defined by Name (or user type), User Name, and encrypted password.

Name (type): oaUser User Name: pmacadmin

PMAC uses these credentials to communicate with OAs for all enclosures it monitors. Therefore, all active OAs must be updated to use the same new credentials. The **updateCredentials** script is used to match the credentials the PMAC uses. Lastly, all enclosures already provisioned in the PMAC must be rediscovered.

- To update the credentials on the OA's, log into the active OA GUI. On the left hand side of the OA GUI, navigate to **Users/Authentication > Local Users > pmacadmin**. After supplying the new password, click **Update User**.
- To update the credentials on the PMAC, execute the following on the PMAC shell:


```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=oaUser
```
- To rediscover an enclosure already provisioned in the PMAC inventory, log into the PMAC GUI and navigate to **Hardware > System Inventory > Cabinet XXX > Enclosure XXXXX** and click **Rediscover Enclosure**.

Name (type): msa User Name: manage

All SAN controllers the PMAC is expected to communicate with must be updated to have the new credentials. The **updateCredentials** script is used to match credentials the PMAC uses.

- To update the credentials, log into Fibre Channel Disk Controller via ssh as a manage user. Then execute:


```
# set password manage
```
- To update the credentials on the PMAC, execute the following in the UI:


```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=msa
```

Name (type): tpdPlatCfg User name: platcfg

The tpdPlatCfg credentials are used to communicate with the TPD tprProvd soap interface and to log into the Platcfg utility when not already logged in as root. The Storage Configuration functionality on the PMAC uses the TPD platcfg credentials when communicating with its TVOE host. If the tpdPlatcfg credentials are changed on the PMAC TPD OS, it must also be changed on the PMAC application using this command.

To update the Linux tpdPlatcfg credentials on the PMAC, log into the PMAC shell with the root credentials and execute:

```
$ passwd platcfg
```

- To update the credentials on the PMAC, execute the following in the shell:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=tpdPlatCfg
```

Name (type): tvoeUser User Name: tvoeadmin

TVOE administrator passwords need to be changed for all TVOE hosts the PMAC is expected to communicate with. The script **updateCredentials** should be used to match the credentials PMAC uses.

Note: Each time a new TVOE is installed its default password has to be updated to match if the default has been changed.

- To update the credentials, log into the TVOE shell with the root credentials and execute:

```
$ passwd tvoeadmin
```

- To update the credentials on the PMAC, execute the following on the PMAC shell:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=tvoeUser
```

Name (type): backupPassword User Name: backupPassword

PMAC backup images are encrypted. The passphrase to encrypt the backup files may be changed. This only changes the encryption for future backups; prior backups cannot be restored without changing to the original pass phrase as shown below. A restore task that fails with a "Failed to decrypt backup file" reason is an indication of this condition.

- To update the passphrase on a PMAC, execute the following in the shell:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=backupPassword
```

Name (type): remoteBackupUser User Name: pmacop

If pmacop credentials are changed on a redundant PMAC, the updateCredentials should be used to match credentials the primary PMAC uses.

- To update the credentials on a redundant PMAC, log into the redundant PMAC shell with the root credentials and execute:

```
$ passwd pmacop
```

- To update the credentials on the primary PMAC, execute the following in primary PMAC shell:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=remoteBackupUser
```

Name (type): oobUser User Name: root

These credentials are used to communicate with the iLO of RMS, when no other credentials have been specified when the RMS was provisioned in PMAC. So the user has the option to modify this default password, or the RMS can be edited/added in the GUI with its specific credentials.

- To update the credentials on an RMS iLO, log into the iLO GUI and navigate to **Administration > User Administration**. Check the box next to root password and click the **Edit** button. After the password is changed, click **Update User**.
- To modify the default oobUser credentials on the PMAC, execute the following in the shell:


```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=oobUser
```
- To add a RMS to PMAC system inventory with its unique iLO password, refer to 9.15 Add Rack Mount Server to the PMAC System Inventory.
- To edit iLO password of a specific RMS already in PMAC system inventory, refer to 9.16 Edit Rack Mount Server in the PMAC System Inventory.

tpdProvd

The tpdProvd credentials are used to allow tpdProvd communication between the PMAC and servers on its control network. The procedure for updating the tpdProvd password has changed as of PMAC 66.5.0. The user can now enter multiple passwords which can be matched to one or more individual servers. The update of the password on the PMAC does not use the **updateCredentials** script in this case. It uses two new commands under the pmacadm cli interface: addProvdCredentials and deleteProvdCredentials.

Expected Behaviors

1. If a tpdProvd password is changed on a non-discovered provisioned server (seen in the **Main Menu->Software->Software Inventory** page but no data is associated to it) on both the server side and the **PMAC side**, after a few minutes, the IPv6 address will appear in the "Address" field and the server will self discover. The server can also be fully discovered if that server is selected in the grid and the **Rediscover** button is selected.
2. If a tpdProvd password is changed on an existing discovered server but not updated on the **PMAC side**, that server will remain discovered in the **Main Menu->Software->Software Inventory** page until a **sentry restart** is performed. Once performed, the server will no longer show as discovered in the Software Inventory page. Once the tpdProvd password has been updated on the **PMAC**, the behavior in number 1 will occur.

Procedure

- a. Update the password on a given server or group of servers (assuming all passwords are the same for the group) either using the linux **passwd** command on the server(s) or by some other means.
- b. From a PMAC shell, use the following command to add the password(s) to the PMAC database and update the PMAC messaging interface. This command will prompt the user for the password and echo asterisks as characters are entered.

Note: --flushBAs can be set to "no" if entering multiple passwords and set to "yes" on the last password add. If --flushBAs is not set to "yes" on the last password entry, a **sentry restart** must be performed on the PMAC to flush out all the Broker Agents (server interfaces) in the PMAC messaging system and rebuild them using the new passwords.

```
/usr/bin/sudo /usr/TKLC/smac/bin/pmacadm addProvdCredentials --
flushBAs=yes
```

- c. The new password can be verified using the following command (this should return a valid response with a password. If it fails, there may be a tpdProvd password mismatch issue between the PMAC and the server):

```
/usr/bin/sudo /usr/TKLC/smac/bin/pmaccli getHostCommStr --
ip=<ipv4 address of the server> --accessType=ro
```

- d. If a password must be removed (and the exact spelling of the password is known), it can be deleted from the PMAC database and messaging system using the following command (again note that the user is prompted for the password):

```
/usr/bin/sudo /usr/TKLC/smac/bin/pmacadm deleteProvdCredentials -
-flushBAs=yes
```

Appendix H.2 PMAC GUI Account Credentials

Modification of any of the PMAC GUI accounts has no system impact. The PMAC GUI users can be updated by logging into the PMAC GUI as guiadmin, and navigating to **Administration > Access Control > Users**. Select the user from the list of users and click **Update Password**.

This will present a Change Password page where the new password must be typed twice. If the password is to be changed on the next login, the **Force password change on next login** checkbox can be set. It defaults to set.

Appendix H.3 PMAC Linux User Account Credentials

Modification of any PMAC Linux user account has no system impact with the exception of the **pmacop** user and **admusr** credentials. If pmacop credentials are changed on a redundant PMAC, use the updateCredentials to match the credentials the primary PMAC uses. If admusr credentials are changed after configuration of the netconfig repository, then delete netconfig services and re-add using the new credentials.

To update the pmacop (or any other Linux user - see list below) credentials on a redundant PMAC, log into the redundant PMAC shell with the pmacop credentials and execute:

```
$ passwd
```

To update the pmacop credentials the primary PMAC uses to communicate with the redundant PMAC, execute the following in primary PMAC shell:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=pmacop
```

The current list of linux users (not including nologin users) added by the PMAC are as follows:

- awadmin:Appworks admin user:/home/awadmin:/bin/bash
- pmacuser:PMAC User:/home/pmacuser:/bin/bash
- pmacadmin:PMAC Administrative User:/home/pmacadmin:/bin/bash
- pmacop:PMAC Operator User:/home/pmacop:/bin/bash
- pmacftpusr:/var/TKLC/smac/image/isoimages//home/smacftpusr:/usr/bin/rsch

To update the pmacop credentials on a redundant PMAC, log into the redundant PMAC UI with the pmacop credentials and execute:

```
$ passwd
```

To update the pmacop credentials the primary PMAC uses to communicate with the redundant PMAC, execute the following in primary PMAC UI:

```
$ sudo /usr/TKLC/smac/bin/updateCredentials --type=pmacop
```

Appendix H.4 NetConfig Manager Password

The netConfig repository stores access credentials for network devices and platform services. To secure these credentials, they are stored as encrypted strings. Platform 7.0 implemented new cryptographic support. The pass phrase used to encrypt this data can be changed by the user through the netConfig API:

```
$ sudo netConfig --repo setPassword
```

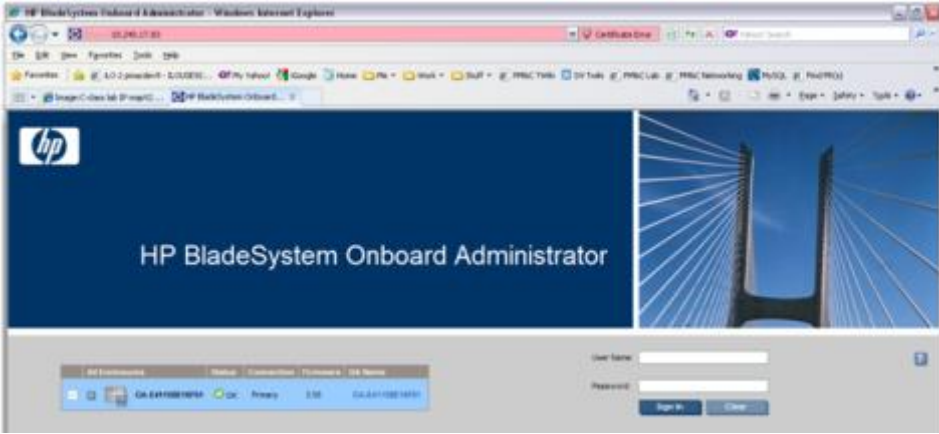
The preceding command prompts for a new pass phrase. It re-encrypts the credentials and stores the pass phrase to a file for use by netConfig.

Appendix I. Disable SNMP on the OA

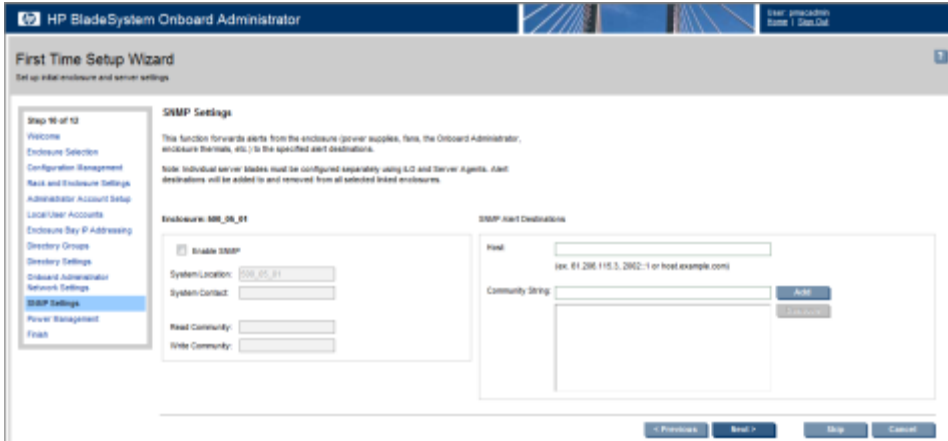
This procedure disables SNMP on the OA.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 119. Disable SNMP on the OA

| Step | Procedure | Results |
|-----------------|---|--|
| <p>1. □</p> | <p>OA GUI: Login</p> | <p>From a web browser, navigate to the OA Bay1 IP address assigned in 7.1 Configure Initial OA IP. <a href="http://<OA_IP>">http://<OA_IP></p> <p>Login as an administrative user. The original password is on a paper card attached to each OA.</p>  |
| <p>2. □</p> | <p>OA GUI: SNMP Settings</p> | <p>Use either the First Time Setup Wizard SNMP Settings menu or the Enclosure Information > Enclosure Settings > SNMP Settings menu.</p> |

Procedure 119. Disable SNMP on the OA

| Step | Procedure | Results |
|--------------------------------|---------------------------------|---|
| 3. <input type="checkbox"/> | OA GUI: SNMP Settings | Unmark the Enable SNMP checkbox.  |

Appendix J. Downgrade Firmware on a 6125G Switch

This procedure downgrades firmware on 6125G enclosure switches when they are found to contain firmware newer than the qualified baseline. See [2] HP Solutions Firmware Upgrade Pack for the target firmware version.

Prerequisite: This procedure assumes the netConfig repository data fill is complete including copying the target firmware to the netConfig server (PMAC).

Note: Do not use this procedure for 6125XLG switches. See Appendix K for the correct procedure for that switch.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 120. Downgrade Firmware on a 6125G Switch

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Active OA: Login | SSH into the active OA and login as the administrative user. <pre>login as: <oa_user> <oa_user>@<oa_ip>'s password: <oa_password></pre> |
| 2. <input type="checkbox"/> | Active OA: Access serial console | Gain serial console access to the switch by executing the following command. Note: Multiple Enter keystrokes are required to gain the switch console prompt. <pre>> connect interconnect <io_bay> [Enter] [Enter] [Enter] Username: <switch_user> [Enter] Password: <switch_password> [Enter] [Enter]</pre> |

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|--|--|---|
| <p>3. <input type="checkbox"/></p> | <p>Switch: Determine firmware</p> | <p>Execute the display version command to determine if a downgrade of the firmware needs to be performed.</p> <pre>> display version HP Comware Platform Software Comware Software, Version 5.20.99, Release 2105 Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P. HP 6125G Blade Switch uptime is 0 week, 2 days, 23 hours, 49 minutes Slot 1 (M): Uptime is 0 weeks,2 days,23 hours,49 minutes HP 6125G Blade Switch with 1 Processor 1024M bytes SDRAM 256M bytes Nand Flash Memory Hardware Version is Ver.B CPLD Version is 003 BootWare Version is 1.07 [SubSlot 0] Back Panel [SubSlot 1] Front Panel</pre> <p>If the firmware is found to be newer than the target firmware, then proceed with the rest of this procedure; otherwise, gracefully exit the switch and PMAC.</p> |
| <p>4. <input type="checkbox"/></p> | <p>Virtual PMAC: Login</p> | <p>SSH into the PMAC and login as admusr.</p> <pre>login as: admusr Password: <admusr_password> Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61 [admusr@<pmac> ~]\$</pre> |
| <p>5. <input type="checkbox"/></p> | <p>Virtual PMAC: Copy firmware</p> | <p>Copy the firmware file to the switch.</p> <pre>\$ sudo /usr/bin/scp 6125-cmw520-r2105.bin <switch_user>@<switch_ip>:/6125-cmw520-r2105.bin <switch_user>@<switch_ip>'s password: <switch_platform_password> 100% 16MB 766.3KB/s 00:21</pre> |
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC: Exit</p> | <p>Gracefully exit from the PMAC SSH session.</p> <pre>\$ logout</pre> |
| <p>7. <input type="checkbox"/></p> | <p>Active OA: Login</p> | <p>If not already connected, ssh into the active OA and login as the administrative user.</p> <pre>login as: <oa_user> <oa_user>@<oa_ip>'s password: <oa_password></pre> |
| <p>8. <input type="checkbox"/></p> | <p>Active OA: Access serial console</p> | <p>If not already connected, gain serial console access to the switch by executing the following command.</p> <p>Note: Multiple Enter keystrokes are required to gain the switch console prompt.</p> <pre>> connect interconnect <io_bay> [Enter] [Enter] [Enter] Username: <switch_user> [Enter] Password: <switch_password> [Enter] [Enter]</pre> |

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|-----------------|---|--|
| <p>9. □</p> | <p>Switch: Reboot switch</p> | <p>Reboot the switch and enter into the extended boot menu by pressing Ctrl+B when prompted.</p> <p>Note: During this process you may be prompted for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.</p> <pre> > reboot Start to check configuration with next startup configuration file, please wait.....DONE!N This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]: N This command will reboot the device. Continue? [Y/N]: Y #May 15 15:03:44:478 2015 HP6125G_IOBAY5 DEVM/1/REBOOT: Reboot device by command. %May 15 15:03:44:570 2015 HP6125G_IOBAY5 DEVM/5/SYSTEM_REBOOT: System is rebooting now. System is starting... Press Ctrl+D to access BASIC BOOT MENU Press Ctrl+T to start memory test Booting Normal Extend BootWare The Extend BootWare is self-decompressing.....Done! [OUTPUT REMOVED] BootWare Validating... Backup Extend BootWare is newer than Normal Extend BootWare,Update? [Y/N] Press Ctrl+B to enter extended boot menu... BootWare password: Not required. Please press Enter to continue. [OUTPUT REMOVED] </pre> |
|-----------------|---|--|

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|------------------|--|--|
| <p>10. □</p> | <p>Switch: Access File Control menu</p> | <p>Select 4 to access the file control from the extend-bootware menu.</p> <pre> ===== <EXTEND-BOOTWARE MENU> ===== <1> Boot System <2> Enter Serial SubMenu <3> Enter Ethernet SubMenu <4> File Control <5> Restore to Factory Default Configuration <6> Skip Current System Configuration <7> BootWare Operation Menu <8> Clear Super Password <9> Storage Device Operation <0> Reboot ===== Ctrl+Z: Access EXTEND-ASSISTANT MENU Ctrl+C: Display Copyright Ctrl+F: Format File System Enter your choice(0-9): 4 </pre> |
|------------------|--|--|

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|---|--|---|
| <p>11. <input type="checkbox"/></p> | <p>Switch: Identify target firmware</p> | <p>Select 1 from the file control menu to list all files and identify the target firmware from the list.</p> <pre> =====<File CONTROL>===== Note:the operating device is flash <1> Display All File(s) <2> Set Application File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 1 Display all file(s) in flash: 'M' = MAIN 'B' = BACKUP 'S' = SECURE 'N/A' = NOT ASSIGNED ===== NO. Size(B) Time Type Name 1 1584 Aug/27/2015 18:41:08 N/A private-data.txt 2 151 Aug/27/2015 18:41:08 N/A system.xml 3 3626 Aug/27/2015 18:41:09 M config.cfg 4 16493888 Aug/20/2015 11:14:44 M+B 6125-cmw520-r2106.bin 5 4 Apr/26/2000 07:00:52 N/A snmpboots 6 16913408 Aug/20/2015 10:56:42 N/A 6125-cmw520-r2112.bin 7 735 Apr/26/2000 12:04:14 N/A hostkey_v3 8 591 Apr/26/2000 12:04:15 N/A serverkey_v3 9 16166 Sep/05/2013 10:17:21 N/A test 10 16053376 Jun/05/2012 10:14:37 N/A ~/6125-cmw520-r2103.bin 11 16479296 Apr/26/2000 10:31:54 N/A ~/6125-cmw520-r2105.bin 12 16493888 Apr/26/2000 10:59:10 N/A ~/6125-cmw520-r2106.bin 13 16479296 Nov/05/2013 23:24:06 N/A ~/2105.bin 14 5361 Jun/25/2013 14:22:05 N/A ~/config.cfg 15 16493888 Nov/05/2013 23:20:13 N/A ~/2106.bin 16 1048519 Aug/27/2015 23:30:55 N/A logfile/logfile.log 17 735 Apr/26/2000 12:05:10 N/A hostkey 18 591 Apr/26/2000 12:05:11 N/A serverkey ===== [OUTPUT REMOVED] </pre> |
|---|--|---|

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|---|---|--|
| <p>12. <input type="checkbox"/></p> | <p>Switch: Set application file type</p> | <p>Select 2 from the file control menu to set the application file type.</p> <pre> =====<File CONTROL>===== Note:the operating device is flash <1> Display All File(s) <2> Set Application File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 2 </pre> |
| <p>13. <input type="checkbox"/></p> | <p>Switch: Select file</p> | <p>Select the firmware file identified in step Error! Reference source not found. and enter the corresponding line number.</p> <p>'M' = MAIN 'B' = BACKUP 'S' = SECURE 'N/A' = NOT ASSIGNED</p> <pre> ===== NO. Size(B) Time Type Name ----- ----- ----- ----- 1 16493888 Aug/20/2015 11:14:44 M+B 6125-cmw520-r2106.bin 2 16913408 Aug/20/2015 10:56:42 N/A 6125-cmw520-r2112.bin 3 16053376 Jun/05/2012 10:14:37 N/A ~/6125-cmw520-r2103.bin 4 16479296 Apr/26/2000 10:31:54 N/A ~/6125-cmw520-r2105.bin 5 16493888 Apr/26/2000 10:59:10 N/A ~/6125-cmw520-r2106.bin 6 16479296 Nov/05/2013 23:24:06 N/A ~/2105.bin 7 16493888 Nov/05/2013 23:20:13 N/A ~/2106.bin 0 Exit ===== Enter file No: <4> </pre> |
| <p>14. <input type="checkbox"/></p> | <p>Switch: Modify file attribute</p> | <p>Select 1 from the file attributes menu to modify the file attribute to +Main.</p> <p>Modify the file attribute:</p> <pre> ===== <1> +Main <2> -Main <3> +Backup <4> -Backup <0> Exit ===== Enter your choice(0-4): 1 This operation may take several minutes. Please wait.... Set the file attribute success! </pre> |

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|---|-------------------------------------|---|
| <p>15. <input type="checkbox"/></p> | <p>Switch: Verify change</p> | <p>Select 1 from the file control menu to verify the file attribute modification by listing the files and inspecting the type attribute for the target firmware. The type attribute on this line should display M:</p> <pre> =====<File CONTROL>===== Note:the operating device is flash <1> Display All File(s) <2> Set Application File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 1 Display all file(s) in flash: 'M' = MAIN 'B' = BACKUP 'S' = SECURE 'N/A' = NOT ASSIGNED NO. Size(B) Time Type Name 1 1584 Aug/27/2015 18:41:08 N/A private-data.txt 2 151 Aug/27/2015 18:41:08 N/A system.xml 3 3626 Aug/27/2015 18:41:09 M config.cfg 4 16493888 Aug/20/2015 11:14:44 B 6125-cmw520-r2106.bin 5 4 Apr/26/2000 07:00:52 N/A snmpboots 6 16913408 Aug/20/2015 10:56:42 N/A 6125-cmw520-r2112.bin 7 735 Apr/26/2000 12:04:14 N/A hostkey_v3 8 591 Apr/26/2000 12:04:15 N/A serverkey_v3 9 16166 Sep/05/2013 10:17:21 N/A test 10 16053376 Jun/05/2012 10:14:37 N/A ~/6125-cmw520-r2103.bin 11 16479296 Apr/26/2000 10:31:54 M ~/6125-cmw520-r2105.bin 12 16493888 Apr/26/2000 10:59:10 N/A ~/6125-cmw520-r2106.bin 13 16479296 Nov/05/2013 23:24:06 N/A ~/2105.bin 14 5361 Jun/25/2013 14:22:05 N/A ~/config.cfg 15 16493888 Nov/05/2013 23:20:13 N/A ~/2106.bin 16 1048519 Aug/27/2015 23:30:55 N/A logfile/logfile.log 17 735 Apr/26/2000 12:05:10 N/A hostkey 18 591 Apr/26/2000 12:05:11 N/A serverkey ===== </pre> |
|---|-------------------------------------|---|

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|------------------|----------------------------|---|
| <p>16. □</p> | <p>Switch: Exit</p> | <p>Select 0 from the file control menu to Exit to the main menu.</p> <pre> ===== <File CONTROL> ===== Note:the operating device is flash <1> Display All File(s) <2> Set Application File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 0 </pre> |
|------------------|----------------------------|---|

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|------------------|---------------------------------------|---|
| <p>17. □</p> | <p>Switch: Boot the system</p> | <p>Select 1 from the extend-bootware menu to Boot the system. Note: Do NOT select reboot by choosing 0! Note: During this process you may be asked for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.</p> <pre> ===== <EXTEND-BOOTWARE MENU> ===== <1> Boot System <2> Enter Serial SubMenu <3> Enter Ethernet SubMenu <4> File Control <5> Restore to Factory Default Configuration <6> Skip Current System Configuration <7> BootWare Operation Menu <8> Clear Super Password <9> Storage Device Operation <0> Reboot ===== Ctrl+Z: Access EXTEND-ASSISTANT MENU Ctrl+C: Display Copyright Ctrl+F: Format File System Enter your choice(0-9): 1 Starting to get the main application file--flash:/~/6125-cmw520-r2105.bin!..... The main application file is self-decompressing..... [OUTPUT REMOVED]Done! System application is starting... User interface aux0 is available. Press ENTER to get started. Login authentication Username: </pre> |
|------------------|---------------------------------------|---|

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|------------------|-----------------------------|---|
| <p>18. □</p> | <p>Switch: Login</p> | <p>Log back into the switch and verify the firmware version by executing the display version command.</p> <p>Note: You may have to press Enter multiple times after authenticating to land on the switch prompt.</p> <pre> Username: username Password: password #Aug 28 09:29:09:694 2015 HP6125g_sanity SHELL/4/LOGIN: Trap 1.3.6.1.4.1.25506.2.2.1.1.3.0.1:plat login from Console %Aug 28 09:29:09:819 2015 HP6125g_sanity SHELL/5/SHELL_LOGIN: plat logged in from aux0. > display version HP Comware Platform Software Comware Software, Version 5.20.99, Release 2105 Copyright (c) 2010-2013 Hewlett-Packard Development Company, L.P. HP 6125G Blade Switch uptime is 0 week, 0 day, 0 hour, 9 minutes [OUTPUT REMOVED] </pre> |
|------------------|-----------------------------|---|

Procedure 120. Downgrade Firmware on a 6125G Switch

| | | |
|---|--|--|
| <p>19. <input type="checkbox"/></p> | <p>Switch: Disconnect from the switch</p> | <p>Gracefully disconnect from the switch serial console by pressing Ctrl + _ (Control + Shift + Underscore). > '<Ctrl>_' (Control + Shift + Underscore)</p> <p>-----</p> <p>Command: D)isconnect, C)hange settings, send B)reak, E)xit command mode X)modem</p> <p>send > D</p> <p>-----</p> <p>D</p> |
| <p>20. <input type="checkbox"/></p> | <p>Active OA: Logout</p> | <p>Log out of the OA. > logout</p> |

Appendix K. Downgrade Firmware on a 6125XLG Switch

This procedure downgrades the 6125XLG enclosure switches when they are found to contain firmware newer than the qualified baseline. See [2] HP Solutions Firmware Upgrade Pack for the target firmware version.

Prerequisite: This procedure assumes the netConfig repository data fill is complete including copying the target firmware to the netConfig server (PMAC).

Note: Do not use this procedure for 6125 switches. See Appendix J for the correct procedure for that switch.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|--|--|--|
| <p>1. <input type="checkbox"/></p> | <p>Active OA: Login</p> | <p>SSH into the active OA and login as the administrative user:</p> <pre>login as: <oa_user> <oa_user>@<oa_ip>'s password: <oa_password></pre> |
| <p>2. <input type="checkbox"/></p> | <p>Active OA: Access serial console</p> | <p>Gain serial console access to the switch by executing the following command.</p> <p>Note: Multiple Enter keystrokes are required to gain the switch console prompt.</p> <pre>> connect interconnect <io_bay> Username: <switch_user> Password: <switch_password></pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|--|--|---|
| <p>3. <input type="checkbox"/></p> | <p>Switch: Determine firmware</p> | <p>Execute the display version command to determine if a downgrade of the firmware needs to be performed.</p> <pre>> display version HP Comware Software, Version 7.1.045, Release 2403 Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P. HP 6125XLG Blade Switch uptime is 0 weeks, 0 days, 0 hours, 1 minute Last reboot reason : Power on Boot image: flash:/6125xlg-cmw710-boot-r2403.bin Boot image version: 7.1.045P08, Release 2403 Compiled Mar 06 2014 13:13:45 System image: flash:/6125xlg-cmw710-system-r2403.bin System image version: 7.1.045, Release 2403 Compiled Mar 06 2014 13:13:57</pre> <p>If the firmware is found to be newer than the target firmware, then proceed with the rest of this procedure; otherwise, gracefully exit the switch and PMAC.</p> |
| <p>4. <input type="checkbox"/></p> | <p>Virtual PMAC: Login</p> | <p>SSH into the PMAC and login as admusr.</p> <pre>login as: admusr Password: <admusr_password> Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61 [admusr@<pmac> ~]\$</pre> |
| <p>5. <input type="checkbox"/></p> | <p>Virtual PMAC: Copy firmware</p> | <p>Copy the firmware file to the switch.</p> <pre>\$ sudo /usr/bin/scp 6125XLG-CMW710-R2403.ipe <switch_user>@<switch_ip>:/6125XLG-CMW710-R2403.ipe <switch_user>@<switch_ip>'s password: <switch_platform_password> 100% 16MB 766.3KB/s 00:21</pre> |
| <p>6. <input type="checkbox"/></p> | <p>Virtual PMAC: Exit</p> | <p>Gracefully exit from the PMAC SSH session.</p> <pre>\$ logout</pre> |
| <p>7. <input type="checkbox"/></p> | <p>Active OA: Login</p> | <p>If not already connected, ssh into the active OA and login as the administrative user.</p> <pre>login as: <oa_user> <oa_user>@<oa_ip>'s password: <oa_password></pre> |
| <p>8. <input type="checkbox"/></p> | <p>Active OA: Access serial console</p> | <p>If not already connected, gain serial console access to the switch by executing the following command.</p> <p>Note: Multiple Enter keystrokes are required to gain the switch console prompt.</p> <pre>> connect interconnect <io_bay> Username: <switch_user> Password: <switch_password></pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|---|--|--|
| <p>9. <input type="checkbox"/></p> | <p>Switch: Reboot switch</p> | <p>Reboot the switch and enter into the extended boot menu by pressing Ctrl+B when prompted.</p> <p>Note: During this process you may be prompted for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.</p> <pre>> reboot Start to check configuration with next startup configuration file, please wait.....DONE!N This command will reboot the device. Current configuration will be lost, save current configuration? [Y/N]: N This command will reboot the device. Continue? [Y/N]: Y Now rebooting, please wait... System is starting... Press Ctrl+D to access BASIC-BOOTWARE MENU... Press Ctrl+T to start heavy memory test Booting Normal Extended BootWare The Extended BootWare is self- decompressing.....Done. [OUTPUT REMOVED] BootWare Validating... Press Ctrl+B to access EXTENDED-BOOTWARE MENU... [OUTPUT REMOVED]</pre> |
| <p>10. <input type="checkbox"/></p> | <p>Switch: Access File Control menu</p> | <p>Select 4 to access the file control from the extend-bootware menu.</p> <pre>=====<EXTEND-BOOTWARE MENU>===== <1> Boot System <2> Enter Serial SubMenu <3> Enter Ethernet SubMenu <4> File Control <5> Restore to Factory Default Configuration <6> Skip Current System Configuration <7> BootWare Operation Menu <8> Clear Super Password <9> Storage Device Operation <0> Reboot ===== Ctrl+Z: Access EXTEND-ASSISTANT MENU Ctrl+C: Display Copyright Ctrl+F: Format File System Enter your choice(0-9): 4</pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|---------------------------------|--|---|
| 11. <input type="checkbox"/> | Switch: Identify target firmware | <p>Select 1 from the file control menu to list all files and identify the target firmware from the list.</p> <p>Note: Two files are identified: A system file and a boot file.</p> <pre> =====<File CONTROL>===== Note:the operating device is flash <1> Display All File(s) <2> Set Application File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 1 Display all file(s) in flash: 'M' = MAIN 'B' = BACKUP 'S' = SECURE 'N/A' = NOT ASSIGNED ===== NO. Size(B) Time Type Name 1 110167 Aug/28/2015 18:05:46 N/A flash:/startup.mdb 2 7388 Aug/28/2015 18:05:46 M flash:/startup.cfg 3 1039 Aug/28/2015 18:05:46 N/A flash:/ifindex.dat 4 252 Jan/27/2011 02:29:27 N/A flash:/.trash/.trashinfo 5 62561280 Aug/19/2015 16:55:55 N/A flash:/6125XLG-CMW710- R2406P03.ipe 6 0 Jan/03/2011 20:20:38 N/A flash:/lauth.dat 7 62660608 Aug/19/2015 17:10:28 N/A flash:/6125XLG-CMW710-R2403.ipe 8 591 Jun/02/2011 17:26:58 N/A flash:/serverkey 9 735 Jun/02/2011 17:26:58 N/A flash:/hostkey 10 536 Jan/27/2011 02:39:29 N/A flash:/versionInfo/version1.dat 11 536 Jan/27/2011 02:36:40 N/A flash:/versionInfo/version0.dat 12 8 Jan/01/2011 00:00:21 N/A flash:/versionInfo/versionCtl.dat 13 536 Aug/19/2015 17:13:37 N/A flash:/versionInfo/version7.dat 14 536 Mar/29/2011 18:38:24 N/A flash:/versionInfo/version5.dat 15 536 Mar/29/2011 18:35:41 N/A flash:/versionInfo/version4.dat 16 536 Aug/19/2015 16:59:08 N/A flash:/versionInfo/version6.dat 17 536 Mar/29/2011 18:24:06 N/A flash:/versionInfo/version2.dat 18 536 Mar/29/2011 18:31:37 N/A flash:/versionInfo/version3.dat 19 536 Jan/27/2011 02:32:46 N/A flash:/versionInfo/version9.dat 20 536 Jan/27/2011 02:25:15 N/A flash:/versionInfo/version8.dat 21 20 Aug/28/2015 18:48:29 N/A flash:/.snmpboots 22 53308416 Aug/19/2015 17:11:52 M flash:/6125xlg-cmw710-system- r24.03. bin </pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|---|---|--|
| | | <pre> 23 10433677 Jan/01/2011 00:06:50 N/A flash:/logfile/logfile.log 24 18 Jan/01/2011 00:00:14 N/A flash:/.pathfile 25 796 Jan/01/2011 00:07:25 N/A flash:/license/DeviceID.did 26 796 Jan/01/2011 00:07:25 N/A flash:/license/history/DeviceID_2011 0101000725.did 27 796 Jan/01/2011 00:00:14 N/A flash:/license/history/DeviceID_2011 0101000014.did 28 805 Jan/01/2011 00:00:18 N/A flash:/license/history/DeviceID_2011 0101000018.did 29 54222848 Aug/19/2015 16:57:16 N/A flash:/6125xlg-cmw710-system- r2406p0 3.bin 30 8331264 Aug/19/2015 16:57:06 N/A flash:/6125xlg-cmw710-boot- r2406p03. bin 31 9345024 Aug/19/2015 17:11:38 M flash:/6125xlg-cmw710-boot- r2403.bin ===== [OUTPUT REMOVED] </pre> |
| <p>12. <input type="checkbox"/></p> | <p>Switch: Set bin file type</p> | <pre> Select 2 from the file control menu to set the bin file type. =====<File CONTROL>===== Note:the operating device is flash <1> Display All File(s) <2> Set Bin File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 2 </pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|---|---|--|
| <p>13. <input type="checkbox"/></p> | <p>Switch: Select file</p> | <p>Select the firmware file identified in step Error! Reference source not found. and enter the corresponding line number. 'M' = MAIN 'B' = BACKUP 'N/A' = NOT ASSIGNED</p> <pre> ===== NO. Size(B) Time Type Name 1 53308416 Aug/19/2015 17:11:52 M flash:/6125xlg-cmw710- system-r2403. bin 2 54222848 Aug/19/2015 16:57:16 N/A flash:/6125xlg-cmw710- system-r2406p 03.bin 3 8331264 Aug/19/2015 16:57:06 N/A flash:/6125xlg-cmw710- boot-r2406p03 03.bin 4 9345024 Aug/19/2015 17:11:38 M flash:/6125xlg-cmw710- boot-r2403.bin 0 Exit ===== Note: Select .bin files. One but only one boot image and system image must be included. Enter file No.(Allows multiple selection): 1 Enter another file No.(0-Finish choice): 4 Enter another file No.(0-Finish choice):0 You have selected: flash:/6125xlg-cmw710-system-r2403.bin flash:/6125xlg-cmw710-boot-r2403.bin </pre> |
| <p>14. <input type="checkbox"/></p> | <p>Switch: Modify file attribute</p> | <p>Select 1 from the file attributes menu to modify the file attribute to +Main. Modify the file attribute:</p> <pre> ===== <1> +Main <2> -Main <3> +Backup <4> -Backup <0> Exit ===== Enter your choice(0-4): 1 This operation may take several minutes. Please wait.... Set the file attribute success! </pre> |
| <p>15. <input type="checkbox"/></p> | <p>Switch: Verify change</p> | <p>Select 1 from the file control menu to verify the file attribute modification by listing the files and inspecting the type attribute for the target firmware. The type attribute on this line should display M.</p> <pre> =====<File CONTROL>===== </pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|------|-----------|--|
| | | <pre> Note:the operating device is flash <1> Display All File(s) <2> Set Bin File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 1 Display all file(s) in flash: 'M' = MAIN 'B' = BACKUP 'N/A' = NOT ASSIGNED NO. Size(B) Time Type Name 1 110167 Aug/28/2015 18:05:46 N/A flash:/startup.mdb 2 7388 Aug/28/2015 18:05:46 M flash:/startup.cfg 3 1039 Aug/28/2015 18:05:46 N/A flash:/ifindex.dat 4 252 Jan/27/2011 02:29:27 N/A flash:/.trash/.trashinfo 5 62561280 Aug/19/2015 16:55:55 N/A flash:/6125XLG-CMW710-R2406P03.ipe 6 0 Jan/03/2011 20:20:38 N/A flash:/lauth.dat 7 62660608 Aug/19/2015 17:10:28 N/A flash:/6125XLG-CMW710-R2403.ipe 8 591 Jun/02/2011 17:26:58 N/A flash:/serverkey 9 735 Jun/02/2011 17:26:58 N/A flash:/hostkey 10 536 Jan/27/2011 02:39:29 N/A flash:/versionInfo/version1.dat 11 536 Jan/27/2011 02:36:40 N/A flash:/versionInfo/version0.dat 12 8 Jan/01/2011 00:00:21 N/A flash:/versionInfo/versionCtl.dat 13 536 Aug/19/2015 17:13:37 N/A flash:/versionInfo/version7.dat 14 536 Mar/29/2011 18:38:24 N/A flash:/versionInfo/version5.dat 15 536 Mar/29/2011 18:35:41 N/A flash:/versionInfo/version4.dat 16 536 Aug/19/2015 16:59:08 N/A flash:/versionInfo/version6.dat 17 536 Mar/29/2011 18:24:06 N/A flash:/versionInfo/version2.dat 18 536 Mar/29/2011 18:31:37 N/A flash:/versionInfo/version3.dat 19 536 Jan/27/2011 02:32:46 N/A flash:/versionInfo/version9.dat 20 536 Jan/27/2011 02:25:15 N/A flash:/versionInfo/version8.dat 21 20 Aug/28/2015 18:48:29 N/A flash:/.snmpboots 22 53308416 Aug/19/2015 17:11:52 M flash:/6125xlg-cmw710-system-r2403.bin 23 10433677 Jan/01/2011 00:06:50 N/A flash:/logfile/logfile.log 24 18 Jan/01/2011 00:00:14 N/A flash:/.pathfile 25 796 Jan/01/2011 00:07:25 N/A flash:/license/DeviceID.did 26 796 Jan/01/2011 00:07:25 N/A flash:/license/history/DeviceID_20110101000 725.did 27 796 Jan/01/2011 00:00:14 N/A flash:/license/history/DeviceID_20110101000 014.did 28 805 Jan/01/2011 00:00:18 N/A </pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|------------------|----------------------------|---|
| | | <pre>flash:/license/history/DeviceID_20110101000 018.did 29 54222848 Aug/19/2015 16:57:16 N/A flash:/6125xlg-cmw710-system- r2406p03 .bin 30 8331264 Aug/19/2015 16:57:06 N/A flash:/6125xlg-cmw710-boot- r2406p03.bin 31 9345024 Aug/19/2015 17:11:38 M flash:/6125xlg-cmw710-boot-r2403.bin =====</pre> |
| <p>16. □</p> | <p>Switch: Exit</p> | <p>Select 0 from the file control menu to Exit to the main menu.</p> <pre>=====<File CONTROL>===== Note:the operating device is flash <1> Display All File(s) <2> Set Application File type <3> Delete File <0> Exit To Main Menu ===== Enter your choice(0-3): 0</pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|------------------|---------------------------------------|---|
| <p>17. □</p> | <p>Switch: Boot the system</p> | <p>Select 1 from the extend-bootware menu to Boot the system. Note: Do NOT select reboot by choosing 0! Note: During this process you may be asked for additional input. Only respond with the input noted in this step; otherwise, let the system time out and continue automatically.</p> <pre> ===== <EXTEND-BOOTWARE MENU> ===== <1> Boot System <2> Enter Serial SubMenu <3> Enter Ethernet SubMenu <4> File Control <5> Restore to Factory Default Configuration <6> Skip Current System Configuration <7> BootWare Operation Menu <8> Clear Super Password <9> Storage Device Operation <0> Reboot ===== Ctrl+Z: Access EXTEND-ASSISTANT MENU Ctrl+C: Display Copyright Ctrl+F: Format File System Enter your choice(0-9): 1 Loading the main image files... Loading file flash:/6125xlg-cmw710-system-r2403.bin.....Done. Loading file flash:/6125xlg-cmw710-boot-r2403.bin.....Done. Image file flash:/6125xlg-cmw710-boot-r2403.bin is self-decompressing..... [OUTPUT REMOVED]Done! System application is starting... User interface aux0 is available. Press ENTER to get started. Login authentication Username: </pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|---------------------------------|----------------------|--|
| 18. <input type="checkbox"/> | Switch: Login | <p>Log back into the switch and verify the firmware version by executing the display version command.</p> <p>Note: You may have to press Enter multiple times after authenticating to land on the switch prompt.</p> <pre>login: <switch_user> [Enter] Password: <switch_password> [Enter] [Enter] > display version HP Comware Software, Version 7.1.045, Release 2403 Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P. HP 6125XLG Blade Switch uptime is 0 weeks, 0 days, 0 hours, 1 minute Last reboot reason : Power on Boot image: flash:/6125xlg-cmw710-boot-r2403.bin Boot image version: 7.1.045P08, Release 2403 Compiled Mar 06 2014 13:13:45 System image: flash:/6125xlg-cmw710-system-r2403.bin System image version: 7.1.045, Release 2403 Compiled Mar 06 2014 13:13:57 [OUTPUT REMOVED]</pre> |

Procedure 121. Downgrade Firmware on a 6125XLG Switch

| Step | Procedure | Results |
|---------------------------------|--|--|
| 19. <input type="checkbox"/> | Switch: Disconnect from the switch | Gracefully disconnect from the switch serial console by pressing Ctrl + _ (Control + Shift + Underscore). <pre>> '<Ctrl>_' (Control + Shift + Underscore) ----- Command: D)isconnect, C)hange settings, send B)reak, E)xit command mode X)modem send > D ----- D [Enter]</pre> |
| 20. <input type="checkbox"/> | Active OA: Logout | Log out of the OA. <pre>> logout</pre> |

Appendix L. Change Switch Passwords (netConfig)

This procedure changes switch passwords using netConfig. This updates the passwords in both the repository and on the devices.

This procedure assumes the netConfig repository data fill is complete and the devices have been previously added. If netConfig was not used to configure the switch originally, do not use this procedure.

Caution: This operation should be scheduled with the customer. Executing these commands as stated does not cause a service interruption. The switches are not rebooted or initialized; however, as with all in-service operations, caution should be taken.

At any time, you can view the contents of the netConfig repository by executing the following command on the netConfig Server:

- For switches, use the command: `sudo /usr/TKLC/plat/bin/netConfig --repolistDevices`

Users can run the above command to confirm that the target devices have already been configured. Duplicate entries cannot be added; if changes to a device repository entry are required, use the editDevice command.

Terminology

The term **netConfig server** refers to the entity where netConfig is executed. This may be a virtualized or physical environment. **Management server** may also accurately describe this location, but has been historically used to describe the physical environment while **Virtual PMAC** was used to describe the virtualized netConfig server. Use of the term **netConfig server** to describe dual scenarios of physical and virtualized environments allow for future simplification of network configuration procedures.

Steps within this procedure and subsequent procedures that require this procedure may refer to variable data indicated by text within <>. Fill in these worksheets based on NAPD, and refer back to these tables for the proper value to insert depending on your system type.

| Variable | Value |
|--|-------|
| <netConfig_server_mgmt_IP_address> | |
| <switch_hostname> From NAPD or output from <code>listDevices</code> command | |
| <cleartext_password> | |

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 122. Change Switch Passwords (netConfig)

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | netConfig Server: SSH into the netConfig server | SSH into the netConfig server and authenticate as admusr: <pre>login as: admusr [Enter] Password: <admusr_password> [Enter] Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61 [admusr@<pmac> ~]\$</pre> |
| 2. <input type="checkbox"/> | netConfig Server: Confirm device | Confirm the device is listed in the repository by executing the following command: <pre>\$ sudo /usr/TKLC/plat/bin/netConfig --repo listDevices</pre> Take note of the target device name. This is referred to as the variable <switch_hostname> in subsequent steps. |

Procedure 122. Change Switch Passwords (netConfig)

| Step | Procedure | Results |
|--------------------------------|---|---|
| 3. <input type="checkbox"/> | netConfig Server: Change password | <p>For device types 4948, 4948E, 4948E-F, or 3020:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=<switch_hostname> setPassword type=<console login privileged> password=<cleartext_password>; history -d \$ (history 1)</pre> <p>For device types 6120, 6125G, or 6125XLG:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netConfig -- device=<switch_hostname> setPassword password=<cleartext_password>; history -d \$(history 1)</pre> <p>Note: The appended part of the command, <code>; history -d \$(history 1)</code>, deletes the history so the password is not observable in cleartext. If this is not desirable you may omit this part of the command and resolve the risk manually.</p> |
| 4. <input type="checkbox"/> | netConfig Server: Logout | <p>Gracefully exit from the netConfig server SSH session:</p> <pre>\$ logout</pre> |

Appendix M. Uninstall Symantec NetBackup Client

This procedure uninstalls the Symantec NetBackup client from a server with an OS based on TPD or TVOE.

Note: If you are attempting to uninstall a failed Symantec NetBackup client installation or upgrade, do not use this procedure. This procedure should only be used when the initial Symantec NetBackup client installation, or subsequent upgrade, was successful.

Prerequisites:

- The TPD NetBackup RPM has been installed on the server.
- The contents of the NetBackup client configuration file are known if one exists. Depending on the version of NetBackup, a configuration file may not exist.
- The firewall rules implementation is known. Depending on the application, the implementation of firewall rules vary. Do not proceed without understanding the appropriate steps to remove the rules for your application. Reference the documentation for your specific application. The steps presented in this procedure are for a TVOE server and may not apply to a TPD application server.
- The server health checks return no issues.

In this procedure, target server refers to the TPD or TVOE server where the NetBackup client is installed. In the case of TPD, this is the application server. In the case of TVOE, this is the base server hosting the application virtual machines.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 123. Uninstall Symantec NetBackup Client

| Step | Procedure | Results |
|--------------------------------|---------------------|--|
| 1. <input type="checkbox"/> | Back up application | Back up your application as described in your application documentation. Take care not to use NetBackup since the NetBackup client is being removed from the server. |

Procedure 123. Uninstall Symantec NetBackup Client

| Step | Procedure | Results | | | | | | | | | | | | |
|--------------------------------|---|--|--------------------------|-----------------|----------|--------|----------|---------------|--------|--|---------------|-------------------|--|--------------------------------------|
| 2. <input type="checkbox"/> | Target Server: Login | SSH into the server and login as admusr . <pre>login as: admusr Password: <admusr_password> Last login: Fri Aug 28 12:09:06 2015 from 10.75.8.61 [admusr@<target_server> ~]\$</pre> | | | | | | | | | | | | |
| 3. <input type="checkbox"/> | Target Server: Determine the NetBackup client version | Determine the NetBackup client version by inspecting the version file: <pre>[admusr@<target_server> ~]\$ sudo /bin/cat /usr/opensv/netbackup/bin/version NetBackup-RedHat2.6.18 7.6.0.1 [admusr@<target_server> ~]\$</pre> | | | | | | | | | | | | |
| 4. <input type="checkbox"/> | Target Server: Determine packages installed and services configured | Determine the NetBackup client packages installed and services configured on the server by inspecting the client profile configuration file. For some versions of NetBackup, a configuration file is not used and does not exist. If your installation does not use a client profile file, refer to Table 2 for your specific release. Table 2. Installed Packages and Services for NetBackup Client 7.0, 7.1, 7.5, and 7.7 <table border="1" data-bbox="501 894 1443 1388"> <thead> <tr> <th>NetBackup Client Version</th> <th>Packages (RPMs)</th> <th>Services</th> </tr> </thead> <tbody> <tr> <td>NB 7.0</td> <td>VRTS pbx</td> <td>RC: netbackup</td> </tr> <tr> <td>NB 7.1</td> <td>SYMCpdddea SYMCnbjre SYMCnbjava SYMCnbclt VRTS pbx</td> <td>RC: netbackup</td> </tr> <tr> <td>NB 7.5 and NB 7.7</td> <td>SYMCpdddea SYMCnbjre SYMCnbjava SYMCnbclt VRTS pbx</td> <td>RC: netbackup RC: vxpbx_exchanged</td> </tr> </tbody> </table> Note: The client profile configuration file includes the client version in the name. For example, NB7601.conf where 7601 represents the client version number with the periods removed. In this example, version 7.6.0.1 is used. Inspect the client profile configuration file. <pre>[admusr@<target_server> ~]\$ sudo /bin/cat /usr/TKLC/plat/etc/netbackup/profiles/NB7601.conf VERSION=7.6.0.1 RPMs="SYMCpdddea, SYMCnbjre, SYMCnbjava, SYMCnbclt, VRTSpbx" RC_SERVICES="netbackup, vxpbx_exchanged"</pre> | NetBackup Client Version | Packages (RPMs) | Services | NB 7.0 | VRTS pbx | RC: netbackup | NB 7.1 | SYMCpdddea SYMCnbjre SYMCnbjava SYMCnbclt VRTS pbx | RC: netbackup | NB 7.5 and NB 7.7 | SYMCpdddea SYMCnbjre SYMCnbjava SYMCnbclt VRTS pbx | RC: netbackup RC: vxpbx_exchanged |
| NetBackup Client Version | Packages (RPMs) | Services | | | | | | | | | | | | |
| NB 7.0 | VRTS pbx | RC: netbackup | | | | | | | | | | | | |
| NB 7.1 | SYMCpdddea SYMCnbjre SYMCnbjava SYMCnbclt VRTS pbx | RC: netbackup | | | | | | | | | | | | |
| NB 7.5 and NB 7.7 | SYMCpdddea SYMCnbjre SYMCnbjava SYMCnbclt VRTS pbx | RC: netbackup RC: vxpbx_exchanged | | | | | | | | | | | | |

Procedure 123.Uninstall Symantec NetBackup Client

| Step | Procedure | Results |
|---------------------------------|---|---|
| 5. <input type="checkbox"/> | Target Server: Stop all NetBackup processes | Stop the Symantec NetBackup client services identified in step Error! eference source not found. This example stops the services for NetBackup version 7.6.0.1. <pre>[admusr@<target_server> ~]\$ sudo service netbackup stop stopping the NetBackup Deduplication Multi-Threaded Agent stopping the NetBackup Discovery Framework stopping the NetBackup client daemon stopping the NetBackup network daemon [admusr@<target_server> ~]\$ sudo service vxpbx_exchanged stop Stopped Symantec Private Brach Exchange</pre> |
| 6. <input type="checkbox"/> | Target Server: Verify the processes stopped | Verify all NetBackup processes are stopped. No output is expected. <pre>[admusr@<target_server> ~]\$ sudo /usr/opensv/netbackup/bin/bpps</pre> |
| 7. <input type="checkbox"/> | Target Server: Ensure directory is not already in use | Ensure the directory to which the NetBackup LV is mounted is not already in use. This is a precautionary step. <pre>[admusr@<target_server> ~]\$ cd ~</pre> |
| 8. <input type="checkbox"/> | Target Server: Delete services | Delete the NetBackup services identified in the client profile from step Error! eference source not found. In this example, the NetBackup client services are netbackup and vxpbx_exchanged. <pre>[admusr@<target_server> ~]\$ sudo /usr/TKLC/plat/bin/service_conf del netbackup [admusr@<target_server> ~]\$ sudo /usr/TKLC/plat/bin/service_conf del vxpbx_exchanged</pre> |
| 9. <input type="checkbox"/> | Target Server: Reconfigure services | Reconfigure the server services after the deletion: <pre>[admusr@<target_server> ~]\$ sudo /usr/TKLC/plat/bin/service_conf reconfig</pre> |
| 10. <input type="checkbox"/> | Target Server: xxx | Uninstall the NetBackup client packages identified in the client profile from step Error! Reference source not found. In this example the NetBackup client ackages are SYMCnbclt, SYMCnbjava, SYMCnbjre, SYMCpddea, and VRTSpxb. Note: Warnings can be ignored. <pre>[admusr@<target_server> ~]\$ sudo rpm -ev SYMCnbclt SYMCnbjava SYMCnbjre SYMCpddea VRTSpxb warning: erase unlink of /opt/VRTSpxb/lib/libvxicu18n.so.6 failed: No such file or directory warning: erase unlink of /opt/VRTSpxb/bin/vxpbxcfg failed: No such file or directory Starting SYMCpddea postremove script. Removing link /opt/pdag Removing link /opt/pdshared Removing /opt/pdde directory. Removing link /usr/opensv/lib/ost-plugins/libstspipd.so Removing link /usr/opensv/lib/ost-plugins/libstspipdMT.so Removing PDDE installation directory. SYMCpddea postremove script done!</pre> |

Procedure 123. Uninstall Symantec NetBackup Client

| Step | Procedure | Results |
|---------------------------------|---|---|
| 11. <input type="checkbox"/> | Target Server: Verify removal of client RPMs | Verify the removal of the NetBackup client RPMs. In this example the NetBackup client RPMs are: SYMCnbclt, SYMCnbjava, SYMCnbjre, SYMCPddea, and VRTSpxb. No output is expected. <pre>[admusr@<target_server> ~]\$ sudo rpm -qa egrep "SYMCnbclt SYMCnbjava SYMCnbjre SYMCPddea VRTSpxb"</pre> |
| 12. <input type="checkbox"/> | Target Server: Clean up directory | Clean up the /etc/rc.d/init.d directory. List any NetBackup client service files that may not have been removed by the uninstall of the client RPMs. In this example the client services are netbackup and vxpbx_exchanged. <pre>[admusr@<target_server> ~]\$ sudo ls -l /etc/rc.d/init.d/netbackup /etc/rc.d/init.d/vxpbx_exchanged</pre> ls: cannot access /etc/rc.d/init.d/vxpbx_exchanged: No such file or directory <pre>-r-x----- 1 root root 22776 Sep 6 16:04 /etc/rc.d/init.d/netbackup</pre> The output of this example shows the netbackup service file was not removed. Delete the service file: <pre>[admusr@<target_server> ~]\$ sudo rm -f /etc/rc.d/init.d/netbackup</pre> |
| 13. <input type="checkbox"/> | Target Server: Identify volume and volume group | Identify the NetBackup logical volume (LV) and volume group (VG). The LV and VG are referenced in later steps. <pre>[admusr@<target_server> ~]\$ sudo lvs</pre> LV VG Attr LSize Pool Origin Data% Meta% Move Log Cpy%Sync Convert netbackup_lv vgroot -wi-ao---- 5.00g plat_root vgroot -wi-ao---- 1.00g plat_tmp vgroot -wi-ao---- 1.00g plat_usr vgroot -wi-ao---- 4.00g plat_var vgroot -wi-ao---- 1.00g plat_var_tklc vgroot -wi-ao---- 4.00g The output shows the NetBackup LV is named netbackup_lv and the VG is vgroot . |
| 14. <input type="checkbox"/> | Target Server: Identify processes using volume | Verify no processes are using the LV identified in the previous step. Use the VG and LV values identified in the previous step. No output is expected. <pre>[admusr@<target_server> ~]\$ sudo /sbin/fuser -m /dev/vgroot/netbackup_lv</pre> |
| 15. <input type="checkbox"/> | Target Server: Unmount device | Unmount /usr/opensv device from the NetBackup LV: <pre>[admusr@<target_server> ~]\$ sudo /bin/umount -l /usr/opensv</pre> |
| 16. <input type="checkbox"/> | Target Server: Remove LV entry | Remove the NetBackup LV entry from /etc/fstab file. <pre>[admusr@<target_server> ~]\$ sudo /bin/sed -i.bak '/netbackup_lv/d' /etc/fstab</pre> |
| 17. <input type="checkbox"/> | Target Server: Check in file | Check the /etc/fstab file into the RCS. <pre>[admusr@<target_server> ~]\$ sudo /usr/TKLC/plat/bin/rcscheck /etc/fstab</pre> |

Procedure 123. Uninstall Symantec NetBackup Client

| Step | Procedure | Results |
|---------------------------------|--|--|
| 18. <input type="checkbox"/> | Target Server: Verify removal of file | Verify the removal of the entry from the /etc/fstab file. Compare the /etc/fstab file to the /etc/fstab.bak backup file. <pre>[admusr@<target_server> ~]\$ sudo /usr/bin/diff /etc/fstab.bak /etc/fstab 19d18 < /dev/vgroot/netbackup_lv /usr/opensv ext4 defaults 1 2</pre> |
| 19. <input type="checkbox"/> | Target Server: Remove backup file | Remove the /etc/fstab.bak file. <pre>[admusr@<target_server> ~]\$ sudo rm -f /etc/fstab.bak</pre> |
| 20. <input type="checkbox"/> | Target Server: Remove volume | Remove the NetBackup LV identified in step Error! Reference source not found . Take care to use the correct volume group. <pre>[admusr@<target_server> ~]\$ sudo /sbin/lvremove -f /dev/vgroot/netbackup_lv</pre> |
| 21. <input type="checkbox"/> | Target Server: Remove client package entries | Execute the command in this step to remove the NetBackup client package entries from the pkgKeep.conf file. The NetBackup client packages were identified in step Error! Reference source not found . If pkgKeep.conf only contains these packages, the pkgKeep.conf file can be removed. In this example, the NetBackup client packages are SYMCnbclt, SYMCnbjava, SYMCnbjre, SYMCpddea, and VRTSpx. <pre>[admusr@<target_server> ~]\$ sudo /bin/sed -i.bak '/SYMCnbclt\ SYMCnbjava\ SYMCnbjre\ SYMCpddea\ VRTSpx/d' /usr/TKLC/plat/etc/upgrade/pkgKeep.conf</pre> |
| 22. <input type="checkbox"/> | Target Server: Verify removal of packages | Verify the removal of the NetBackup client package entries from the pkgKeep.conf file by comparing the pkgKeep.conf to the pkgKeep.conf.bak backup file. <pre>[admusr@<target_server> ~]\$ sudo /usr/bin/diff /usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak /usr/TKLC/plat/etc/upgrade/pkgKeep.conf 1,5d0 < SYMCnbclt < SYMCnbjava < SYMCnbjre < SYMCpddea < VRTSpx</pre> |
| 23. <input type="checkbox"/> | Target Server: Remove backup file | Remove the pkgKeep.conf.bak file. <pre>[admusr@<target_server> ~]\$ sudo rm -f /usr/TKLC/plat/etc/upgrade/pkgKeep.conf.bak</pre> |
| 24. <input type="checkbox"/> | Target Server: Remove configuration file | Remove the client profile configuration file, if one exists. The existence of this file is determined in step Error! Reference source not found . Note: The client profile configuration file includes the client version in the name. For example, NB7601.conf where 7601 represents the client version number with the periods removed. In this example, version 7.6.0.1 is used. <pre>[admusr@<target_server> ~]\$ sudo rm -f /usr/TKLC/plat/etc/netbackup/profiles/NB7601.conf</pre> |

Procedure 123. Uninstall Symantec NetBackup Client

| Step | Procedure | Results |
|---------------------------------|--|--|
| 25. <input type="checkbox"/> | Target Server: Remove script file | Remove the NetBackup client script file. For some versions of NetBackup, a script file is not used and does not exist. Proceed to the next step if this is the case. Note: The client profile configuration file includes the client version in the name. For example, NB7601.conf where 7601 represents the client version number with the periods removed. In this example, version 7.6.0.1 is used. <pre>[admusr@<target_server> ~]\$ sudo rm -f /usr/TKLC/plat/etc/netbackup/scripts/NB7601</pre> |
| 26. <input type="checkbox"/> | Target Server: Remove firewall rules | Remove the firewall rules related to NetBackup. Note: This step varies depending on how the application implemented the firewall rules. The example in this step illustrates the correct steps for a TVOE server. If you are uninstalling NetBackup on a TPD application server, refer to the documentation for your specific application. Remove the iptables and ip6tables firewall rules related to NetBackup on a TVOE server: <pre>[admusr@<target_server> ~]\$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --type=domain --domain=60netbackup --protocol=ipv4</pre> <pre>[admusr@<target_server> ~]\$ sudo /sbin/service iptables restart</pre> <pre>iptables: Setting chains to policy ACCEPT: filter [OK]</pre> <pre>iptables: Flushing firewall rules: [OK]</pre> <pre>iptables: Applying firewall rules: [OK]</pre> <pre>[admusr@<target_server> ~]\$ sudo /usr/TKLC/plat/bin/iptablesAdm delete --type=domain --domain=60netbackup --protocol=ipv6</pre> <pre>[admusr@<target_server> ~]\$ sudo /sbin/service ip6tables restart</pre> <pre>ip6tables: Setting chains to policy ACCEPT: filter [OK]</pre> <pre>ip6tables: Flushing firewall rules: [OK]</pre> <pre>ip6tables: Applying firewall rules: [OK]</pre> |
| 27. <input type="checkbox"/> | Target Server: Remove firewall configuration files | Remove firewall configuration files related to NetBackup. Note: This step varies depending on how the application implemented the firewall rules. The example in this step illustrates the correct steps for a TVOE server. If you are uninstalling NetBackup on a TPD application server, refer to the documentation for your specific application. Remove firewall configuration files related to NetBackup on a TVOE server: <pre>[admusr@<target_server> ~]\$ sudo rm -f /usr/TKLC/plat/etc/iptables/60netbackup.ipt</pre> <pre>[admusr@<target_server> ~]\$ sudo rm -f /usr/TKLC/plat/etc/ip6tables/60netbackup.ipt</pre> |

Procedure 123. Uninstall Symantec NetBackup Client

| Step | Procedure | Results |
|---------------------------------|---|---|
| 28. <input type="checkbox"/> | Target Server: Update hosts file | Update the /etc/hosts file to remove the NetBackup server host using the platcfg utility. Note: If the NetBackup entry in the /etc/hosts file is an alias and you do not want to delete the host, select Delete Alias instead of Delete Host . The rest of the steps remain the same. <ol style="list-style-type: none"> 1. As admusr, execute the sudo su - platcfg command to launch the platcfg utility. 2. Select Network Configuration. 3. Select Modify Hosts File. 4. Select Edit. 5. Select Delete Host. 6. Select the host entry for NetBackup. 7. Select Yes to confirm deletion. 8. Exit out of the platcfg utility. |
| 29. <input type="checkbox"/> | Target Server: Verify server health | No unexpected alarms should display and no missing package files should exist. <pre>[admusr@<target_server> ~]\$ sudo /usr/TKLC/plat/bin/alarmMgr -alarmStatus [admusr@<target_server> ~]\$ sudo rpm -Va</pre> |

Appendix N. Configuring NUMA on pmac-deploy

This appendix explains the new NUMA tuning options added to the pmac-deploy command.

Prerequisites:

- No other manual activity is currently in progress on the TVOE host.
- **syscheck** and **alarmMgr** on the TVOE host show no outstanding issues.
- There is adequate resources to properly deploy the PMAC on the TVOE host.

Assumptions/Limitations:

- Users of these new options must fully understand the use and setting of the numa/vcpu assignments and the affects this can have on the overall performance of the TVOE host, the PMAC, and any VMs that may reside on the same TVOE host.
- When --numa is not entered on the command line, the PMAC will use the numa that the TVOE has reserved CPU(s) on. That is usually 0 but it can be something else. This value is defined in file **/usr/TKLC/tvoe/etc/host_resources.cfg** as a comma separated string with a label called **RESERVED_CPUS**.
- NUMA boundaries cannot be crossed when defining the cpuset.
- If more reserved CPUs are configured in the **/usr/TKLC/tvoe/etc/host_resources.cfg** file than are available on a given NUMA when using the new options on deploy, the configuration will fail.

New Options:

The new options include the following:

--cpuset

This option is a CSV string but can include ranges separated by a dash. It can be optionally combined with the --numa option but is mutually exclusive with the --restrictCPus and --startCpu options given below. It attempts to associate the provided cpuset to the PMAC on the given NUMA. Any duplicate CPUs identified in the cpuset will be removed during the configuration process. The number of CPUs in the cpuset must be equal to or greater than the number of vcpus defined (--vcpus defaults to 1).

Example:

```
--cpuset=1,2,3-5
--numa=0 --cpuset=1,2,3-5
--numa=0 --vcpus=4 --cpuset=1,2,3-5
```

--restrictCpus

This option is a simple Boolean. The presents of this option indicates TRUE. It can be combined optionally with the --numa and --vcpus options. It instructs the pmac-deploy to find CPUs on the given NUMA (first available first served) based on the number of VCPUs defined by the --vcpus option (which is optional and defaults to 1). It then associates them to the PMAC guest on deploy. This option is mutually exclusive with the --cpuset option.

Example:

```
--restrictCpus
--numa=0 --restrictCpus
--numa=0 --vcpus=4 --restrictCpus
```

--startCpu

This option is paired with the --restrictCpus option to instruct the deploy to start its CPU search at the given CPU number on the given NUMA (they are in a sorted list). It is mutually exclusive with all other options in the deploy command.

Example:

```
--restrictCpus --startCpu=2
--numa=0 --vcpus=3 --restrictCpus --startCpu=2
```

Appendix O. Update the PMAC GSOAP Cipher List

This procedure defines the method required to update the PMAC **GSOAP** cipher list and how to verify the update was successful.

Prerequisites:

- The file /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg is present on the system.
- No other PMAC manual activity is currently in progress on the PMAC (for example, IPM, Guest creations, etc.).
- syscheck and alarmMgr on the PMAC show no outstanding issues.

Assumptions/Limitations:

- On upgrades, this file will always be overwritten with the contents of the new file version from the new PMAC release. The old file will be copied into the same directory as pmacgsoap.cfg.rpmnew. If the file ciphers have previously been changed and the user wishes to maintain that change, the user

must manually update/merge the previous contents of the file into the new version created by the upgrade.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 124. Update the PMAC GSOAP Cipher List

| Step | Procedure | Results |
|--------------------------------|---|---|
| 1. <input type="checkbox"/> | PMAC Login | Connect to the PMAC shell and log into the PMAC as admusr. |
| 2. <input type="checkbox"/> | Change to root user | If not logged in as the root user, sudo to the root user. <pre>[admusr@p3Pmac1 ~]# sudo su -</pre> |
| 3. <input type="checkbox"/> | Make Backup copy of Pmac GSOP config file | Make a backup copy of the <code>/usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg</code> file and preserve the current permissions and ownership. <pre>cp -p /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg.backup</pre> |
| 4. <input type="checkbox"/> | Run syscheck and alarmMgr | Make sure syscheck and alarmMgr show no outstanding issues. <pre>[root@p3Pmac1 ~]# syscheck [root@p3Pmac1 ~]# alarmMgr --alarmStatus</pre> |
| 5. <input type="checkbox"/> | Edit the PMAC GSOAP config file | Edit the <code>/usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg</code> file: <pre>[root@p3Pmac1 ~]# cd /usr/TKLC/smac/etc/gsoap [root@p3Pmac1 ~]# vim pmacgsoap.cfg</pre> |
| 6. <input type="checkbox"/> | Update the cipher list | Change/update the line <code>ssl_ciphers=....</code> using vim or vi commands. Add appropriate ciphers to this list. Make sure the format is followed exactly. All ciphers must be separated by a single ":". All protocols which are to be excluded should be prefixed with the "!" character. Note: Currently there is no check for inadvertent special characters as the format for a cipher may change in future releases of openssl. Note: In some cases an invalid cipher may simply get ignored by openssl . Before editing this list make sure the ciphers that are being added are valid and known to openssl . The openssl ciphers -v 'cipher list' command (and other variations) can be used to verify the cipher(s) being added. Details of openssl can be found in numerous places on the Web. One good source is at https://wiki.openssl.org/index.php/Command_Line_Uilities |
| 7. <input type="checkbox"/> | Save pmacgsoap.cfg file | Save the changes made to the pmacgsoap.cfg file. |

Procedure 124. Update the PMAC GSOAP Cipher List

| Step | Procedure | Results |
|--|-------------------------------|--|
| <p>8. <input type="checkbox"/></p> | <p>Check status of sentry</p> | <p>On the PMAC shell the sentryd smacTalk process must be restarted. This action will take down the smacTalk process (and others) and restart them. This restart re-creates the smacTalk process and (among other actions) binds in the GSOAP context, reads the pmacgsoap.cfg file cipher list and binds that into the GSOAP openssl port.</p> <p>First check the status of sentryd. This should show the smacTalk and smacMon processes as "running" with a valid PID number. If the sentry restart command is successful the PID number will change as well as the StartTS.</p> <pre>[root@p3Pmac1 ~]# sentry status sending status command... PMAC Sentry Status ----- sentryd started: Wed Apr 25 13:56:30 2018 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 23115 running Wed Apr 25 13:56:30 2018 1 smacMon 23143 running Wed Apr 25 13:56:30 2018 1 hpiPortAudit 23178 running Wed Apr 25 13:56:30 2018 1 snmpEventHandler 23216 running Wed Apr 25 13:56:30 2018 1 Thu Apr 26 07:55:12 2018 Command Complete.</pre> |
| <p>9. <input type="checkbox"/></p> | <p>Perform sentry restart</p> | <p>Perform a sentry restart.</p> <pre>[root@p3Pmac1 ~]# sentry restart sending restart command... sentryd is shutting down all application software, please wait... sentryd is restarting... Thu Apr 26 07:56:52 2018 Command Complete.</pre> |

Procedure 124.Update the PMAC GSOAP Cipher List

| Step | Procedure | Results |
|---|---|---|
| <p>10. <input type="checkbox"/></p> | <p>Check status of sentry</p> | <p>Immediately issue a sentry status command. If the results of this command is “no response from sentryd” on the first try, this is normal as sentryd has not come back up yet. Issue the command again until either all processes are at the “running state” or smacTalk fails to recover.</p> <pre>[root@p3Pmac1 ~]# sentry status sending status command... no response from sentryd (Timer expired), try command again Thu Apr 26 07:56:04 2018 Command Complete.</pre> <p>The smacTalk and smacMon processes status may show as "in recovery". If this is present issue the sentry status command again a few times until all processes have recovered as "running".</p> <pre>[root@p3Pmac1 ~]# sentry status sending status command... PMAC Sentry Status ----- sentryd started: Thu Apr 26 07:56:58 2018 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk --- in recovery Thu Apr 26 07:56:58 2018 1 smacMon --- not running --- 0 hpiPortAudit --- not running --- 0 snmpEventHandler --- not running --- 0 [root@p3Pmac1 ~]# sentry status sending status command... PMAC Sentry Status ----- sentryd started: Thu Apr 26 07:56:58 2018 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 8544 running Thu Apr 26 07:56:58 2018 1 smacMon 8573 running Thu Apr 26 07:56:58 2018 1 hpiPortAudit 8595 running Thu Apr 26 07:56:58 2018 1 snmpEventHandler 8618 running Thu Apr 26 07:56:58 2018 1 Thu Apr 26 07:57:06 2018 Command Complete.</pre> <p>If the smacTalk process fails to return to a “running” state, proceed to step 12 and come back to 11 when the issues have been resolved.</p> |
| <p>11. <input type="checkbox"/></p> | <p>Remove the backup PMAC GSOAP config file</p> | <p>Remove the backup file if desired at /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg.backup.</p> |

Procedure 124.Update the PMAC GSOAP Cipher List

| Step | Procedure | Results |
|---|--------------------------------------|---|
| <p>12. <input type="checkbox"/></p> | <p>sentry restart failure</p> | <p>If smacTalk encounters a fatal error due to an invalid or unacceptable cipher list, the sentry restart and sentry status output will look like the following:</p> <pre>[root@p3Pmac1 ~]# sentry status sending status command... PMAC Sentry Status ----- sentryd started: Wed Apr 25 12:42:30 2018 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk --- not running --- 2 smacMon 8350 running Wed Apr 25 12:42:30 2018 1 hpiPortAudit 8373 running Wed Apr 25 12:42:30 2018 1 snmpEventHandler 8402 running Wed Apr 25 12:42:30 2018 1</pre> <p>If this problem occurs, look at the smacTalkDbug.log file for some idea as to why it failed. There should be logs based on the following error conditions:</p> <ol style="list-style-type: none"> 1. If the openssl function call SSL_CTX_set_cipher_list returns 0 meaning it could not interpret the provided cipher list. Log: "Unable to add GSOAP SSL cipher list - rc: 0" 2. If the cipher list contained in the pmacgsoap.cfg file is an empty string. Log: "Unable to add GSOAP SSL cipher list - list empty - check file: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg" 3. If the openssl function SSL_CTX_set_cipher_list returns something other than 0 or 1 (new version and not expected to occur). Log: "Unable to add GSOAP SSL cipher list - unknown rc: <unknown rc> - check file: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg" 4. If the pmacgsoap.cfg file is successfully opened but the proper cipher list search string "ssl_ciphers" cannot be found. This string should always be on a separate line beginning at column 0. Log: "Unable to add GSOAP SSL cipher list - unable to find ssl_ciphers - check file: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg" 5. If the pmacgsoap.cfg file is missing or cannot be opened due to inadvertent permission changes. Log: "Unable to open: /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg" |
| <p>13. <input type="checkbox"/></p> | <p>Go to PMAC Logs directory</p> | <p>Change directories to the PMAC log directory:</p> <pre>[root@p3Pmac1 ~]# cd /var/TKLC/smac/logs)</pre> |

Procedure 124. Update the PMAC GSOAP Cipher List

| Step | Procedure | Results |
|---------------------------------|---|--|
| 14. <input type="checkbox"/> | Examine logs or contact next level of support | <p>Edit the smactalkDbug.log file. Go to the bottom of the file (if using vim use shift G). Search up for "cipher" (if using vim enter Esc ?cipher).</p> <p>Span up or down in the logs to follow the flow of the cipher list settings. The first log to look for should contain the text: "Returning cipher list" with the cipher list as given in the /usr/TKLC/smac/etc/gsoap/pmacgsoap.cfg file.</p> <p>If these logs do not fully explain the failure (as in it failed with a return code of 0), The cipher list changes made will have to be validated to make sure what was added is in the correct format and is a valid cipher.</p> <p>If unable to resolve the issue please contact the next level of support.</p> |

Appendix P. Update the TPD-Provd Cipher List

This procedure defines the method required to update the TPD-Provd cipher list and how to verify the update was successful.

Prerequisites:

- The file **/usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf** is present on the system.
- **syscheck** and **alarmMgr** on the **tpdProvd** shows no outstanding issues.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 125. Update the TPD Provd Cipher List

| Step | Procedure | Results |
|--------------------------------|--|--|
| 1. <input type="checkbox"/> | Target Server: Login | SSH into the server and login as admusr . <pre>login as: admusr Password: <admusr_password> [admusr ~]\$</pre> |
| 2. <input type="checkbox"/> | Change to root user | If not logged in as the root user, sudo to the root user. <pre>[admusr ~]# sudo su -</pre> |
| 3. <input type="checkbox"/> | Make Backup copy of tpdProvd config file | Make a backup copy of the /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf file and preserve the current permissions and ownership. <pre>[root ~]# cp -p /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf.backup</pre> |
| 4. <input type="checkbox"/> | Run syscheck and alarmMgr | Make sure syscheck and alarmMgr show no outstanding issues. <pre>[root ~]# syscheck [root ~]# alarmMgr --alarmStatus</pre> |
| 5. <input type="checkbox"/> | Edit the TPD-provd config file | Edit the /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf file: <pre>[root ~]# rcstool co /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf [root ~]# cd /usr/TKLC/plat/etc/tpdProvd/ [root ~]# vim tpdProvd.conf</pre> |

Procedure 125.Update the TPD Provd Cipher List

| Step | Procedure | Results |
|---------------------------------|--------------------------|---|
| 6. <input type="checkbox"/> | Update the cipher list | <p>Change/update the line ssl_cipher=.... using vim or vi commands.</p> <p>Add appropriate ciphers to this list. Make sure the format is followed exactly. All ciphers must be separated by a single ":". All protocols which are to be excluded should be prefixed with the "!" character.</p> <p>Note: Currently there is no check for inadvertent special characters as the format for a cipher may change in future releases of openssl. In some cases adding special characters can cause the addition to fail and generate a fatal error in smacTalk.</p> <p>Note: In some cases an invalid cipher may simply get ignored by openssl. Before editing this list, make sure the ciphers that are being added are valid and known to openssl. The openssl ciphers -v 'cipher list' command (and other variations) can be used to verify the cipher(s) being added. Details of openssl can be found in numerous places on the Web. One good source is at https://wiki.openssl.org/index.php/Command_Line_Uutilities.</p> |
| 7. <input type="checkbox"/> | Save tpdProvd.conf file | Save the changes made to the tpdProvd.conf file. |
| 8. <input type="checkbox"/> | Check status of tpdProvd | <p>On the shell the tpdProvd process must be restarted. This action will take down the tpdProvd process (and others) and restart them. This restart re-creates the tpdProvd process and (among other actions) binds in the tpdProvd context, reads the tpdProvd.conf file cipher list and binds that into the tpdProvd openssl port.</p> <p>First check the status of tpdProvd. This should show the tpdProvd process as "running" with a valid PID number. If the start tpdprovd command is successful the PID number will change</p> <pre data-bbox="574 1144 1089 1276">[root ~]# tpdProvd --status Daemon is running... [root ~] status tpdProvd tpdProvd start/running, process 3008</pre> |
| 9. <input type="checkbox"/> | Restart tpdProvd process | <p>Perform a tpdProvd restart.</p> <pre data-bbox="574 1331 1105 1392">[root ~]# restart tpdProvd tpdProvd start/running, process 29232</pre> |
| 10. <input type="checkbox"/> | Check status of tpdProvd | <p>Immediately issue a tpdprovd --status command. Issue the command again until either all processes are at the running state.</p> <pre data-bbox="574 1480 1019 1612">[root ~]# tpdProvd --status Daemon is running... [root ~] status tpdProvd tpdProvd start/running, process</pre> <p>If the tpdProvd process fails to return to a "running" state, proceed to step 13.</p> |

Procedure 125.Update the TPD Provd Cipher List

| Step | Procedure | Results |
|---------------------------------|--|--|
| 11. <input type="checkbox"/> | Verify if the tpdProvd process is working properly by checking the timezone | Issue a command to verify that the tpdProvd process is properly running. If this command fails to return the timeZone, the cipher-list may be incorrect, go back to step 5 and edit cipher-list again, if the error repeats go to step 13. <pre>[root ~]# tpdProvd -client --noxml -address=127.0.0.1 -ns Time timeZone Login on Remote: platcfg Password of platcfg: <platcfg_password> America/New York</pre> |
| 12. <input type="checkbox"/> | Check in the config file and remove the backup file. Procedure is complete | Check in the config file and remove the backup file: <pre>[root ~]# rcstool ci /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf [root ~]# rm /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf.backup</pre> |
| 13. <input type="checkbox"/> | If help is needed to change the cipher list or tpdProvd does not restart, contact My Oracle Support (MOS). | Restore old version of the config file and restart tpdProvd, then contact Customer Service for help altering the cipher-list. <pre>[root ~]# rsctool restore /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf [root ~]# rcstool unco /usr/TKLC/plat/etc/tpdProvd/tpdProvd.conf [root ~]# initctl restart tpdProvd</pre> |

Appendix Q. Increase the PMAC NetBackup Filesystem Size

This procedure increases the PMAC NetBackup file system to accommodate upgrading to NetBackup 7.7 or greater. Currently, the recommended filesystem size for NetBackup 7.7 is 5GB. This filesystem is mounted to a logical volume maintained on the TVOE host.

Prerequisites:

- There is a volume defined on the TVOE host called <pmac guest name>_netback.img and set to 2GB.
- There is a filesystem on the PMAC guest at /dev/<device_name> mounted to /usr/openv' and sized to 2GB.
- The NetBackup filesystem on the PMAC must be type ext2/3/4.
- This procedure assumes there is an entry in the /etc/fstab file for the mounted /usr/openv filesystem.

Notes:

- The <device_name> used can differ from /dev/vdd. This can be determined by issuing the df -h command on the PMAC before starting this procedure and searching for the /usr/openv NetBackup filesystem. Once NetBackup has been enabled and configured on a PMAC, there should be a softlink defined, called /dev/netbackup, which points to the actual device. Usually this points to /dev/vdd. If that is available then all references to /dev/vdd can be replaced with /dev/netbackup and the user does not have to know what actual device is used for the filesystem. The procedure below assumes this to be true.

- The commands listed below require root access to execute them. `sudo` is used to elevate the user permissions to be able to execute the commands. Any command that is not prefixed with `sudo` does not require elevation to execute.
 - All commands are executed from a PMAC shell or from a TVOE shell.
 - Performing this procedure increases the size of the NetBackup filesystem to 5GB. You can use this procedure to increase the NetBackup volume to any size that can be accommodated by the TVOE host. 5GB is the required size for NetBackup 7.7.
 - Each step in this procedure begins by identifying the target server on which the command is to be executed. In this procedure, commands are executed on either the TVOE host or the PMAC.
 - If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.
- If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 126. Increase the PMAC NetBackup Files System Size

| Step | Procedure | Results |
|--------------------------------|----------------------------|--|
| 1. <input type="checkbox"/> | TVOE Host: Login | Connect to the management server's TVOE host shell and log into the PMAC shell as admusr using ssh. |

Procedure 126. Increase the PMAC NetBackup Files System Size

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|--|------------|------|-------------|-------|------------------|------------|------------|--------|-------------------------|----------|------------|-------------|-----------------------|----------|------------|--------|----------------------------|----------|------------|-------|-----------|--------|------------|---------|-----------|--------|------------|-------|----------|--------|------------|-------|----------|--------|------------|-------|----------|--------|------------|-------|---------|--|---------|----------------------------|---------|----------|---------|--|-----------------|------------|------------------------|--|-----------|-----------|--------|---|---------|----------|------------|----|----------|---|------------|---------|--------------------|------|--------------------|------|--------------|--------|
| <p>2.</p> <p><input type="checkbox"/></p> | <p>TVOE Host: Verify existing volume</p> | <p>Verify the existing TVOE NetBackup volume is set to 2GB.</p> <p>1. Display the logical volume sizes.</p> <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /sbin/lvs</pre> <table border="1"> <thead> <tr> <th>LV</th> <th>VG</th> <th>Attr</th> <th>LSize</th> </tr> </thead> <tbody> <tr> <td><pmac_guest>.img</td> <td>vvguests</td> <td>-wi-ao----</td> <td>50.00g</td> </tr> <tr> <td><pmac_guest>_images.img</td> <td>vvguests</td> <td>-wi-ao----</td> <td>20.00g</td> </tr> <tr> <td><pmac_guest>_logs.img</td> <td>vvguests</td> <td>-wi-ao----</td> <td>10.00g</td> </tr> <tr style="background-color: yellow;"> <td><pmac_guest>_netbackup.img</td> <td>vvguests</td> <td>-wi-ao----</td> <td>2.00g</td> </tr> <tr> <td>plat_root</td> <td>vgroot</td> <td>-wi-ao----</td> <td>768.00m</td> </tr> <tr> <td>plat_swap</td> <td>vgroot</td> <td>-wi-ao----</td> <td>2.00g</td> </tr> <tr> <td>plat_tmp</td> <td>vgroot</td> <td>-wi-ao----</td> <td>1.00g</td> </tr> <tr> <td>plat_usr</td> <td>vgroot</td> <td>-wi-ao----</td> <td>3.00g</td> </tr> <tr> <td>plat_var</td> <td>vgroot</td> <td>-wi-ao----</td> <td>1.00g</td> </tr> </tbody> </table> <p>2. Display the logical volume details.</p> <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /sbin/lvdisplay /dev/vvguests/<pmac_guest>_netbackup.img</pre> <pre>--- Logical volume ---</pre> <table border="1"> <tbody> <tr> <td>LV Path</td> <td>/dev/vvguests/<pmac_guest>_netbackup.img</td> </tr> <tr> <td>LV Name</td> <td><pmac_guest>_netbackup.img</td> </tr> <tr> <td>VG Name</td> <td>vvguests</td> </tr> <tr> <td>LV UUID</td> <td>CWe1N1-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp</td> </tr> <tr> <td>LV Write Access</td> <td>read/write</td> </tr> <tr> <td>LV Creation host, time</td> <td><tvoe_host>, 2016-11-14 10:00:54 -0500</td> </tr> <tr> <td>LV Status</td> <td>available</td> </tr> <tr> <td># open</td> <td>1</td> </tr> <tr style="background-color: yellow;"> <td>LV Size</td> <td>2.00 GiB</td> </tr> <tr> <td>Current LE</td> <td>64</td> </tr> <tr> <td>Segments</td> <td>1</td> </tr> <tr> <td>Allocation</td> <td>inherit</td> </tr> <tr> <td>Read ahead sectors</td> <td>auto</td> </tr> <tr> <td>- currently set to</td> <td>4096</td> </tr> <tr> <td>Block device</td> <td>253:19</td> </tr> </tbody> </table> | LV | VG | Attr | LSize | <pmac_guest>.img | vvguests | -wi-ao---- | 50.00g | <pmac_guest>_images.img | vvguests | -wi-ao---- | 20.00g | <pmac_guest>_logs.img | vvguests | -wi-ao---- | 10.00g | <pmac_guest>_netbackup.img | vvguests | -wi-ao---- | 2.00g | plat_root | vgroot | -wi-ao---- | 768.00m | plat_swap | vgroot | -wi-ao---- | 2.00g | plat_tmp | vgroot | -wi-ao---- | 1.00g | plat_usr | vgroot | -wi-ao---- | 3.00g | plat_var | vgroot | -wi-ao---- | 1.00g | LV Path | /dev/vvguests/<pmac_guest>_netbackup.img | LV Name | <pmac_guest>_netbackup.img | VG Name | vvguests | LV UUID | CWe1N1-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp | LV Write Access | read/write | LV Creation host, time | <tvoe_host>, 2016-11-14 10:00:54 -0500 | LV Status | available | # open | 1 | LV Size | 2.00 GiB | Current LE | 64 | Segments | 1 | Allocation | inherit | Read ahead sectors | auto | - currently set to | 4096 | Block device | 253:19 |
| LV | VG | Attr | LSize | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>.img | vvguests | -wi-ao---- | 50.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>_images.img | vvguests | -wi-ao---- | 20.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>_logs.img | vvguests | -wi-ao---- | 10.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>_netbackup.img | vvguests | -wi-ao---- | 2.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_root | vgroot | -wi-ao---- | 768.00m | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_swap | vgroot | -wi-ao---- | 2.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_tmp | vgroot | -wi-ao---- | 1.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_usr | vgroot | -wi-ao---- | 3.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_var | vgroot | -wi-ao---- | 1.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LV Path | /dev/vvguests/<pmac_guest>_netbackup.img | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LV Name | <pmac_guest>_netbackup.img | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| VG Name | vvguests | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LV UUID | CWe1N1-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LV Write Access | read/write | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LV Creation host, time | <tvoe_host>, 2016-11-14 10:00:54 -0500 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LV Status | available | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| # open | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| LV Size | 2.00 GiB | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Current LE | 64 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Segments | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Allocation | inherit | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Read ahead sectors | auto | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| - currently set to | 4096 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Block device | 253:19 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>3.</p> <p><input type="checkbox"/></p> | <p>PMAC: Verify filesystem</p> | <p>Verify the NetBackup filesystem is set to 2GB.</p> <pre>[admusr@<pmac_guest> ~]\$ /bin/df -h /usr/opencv</pre> <table border="1"> <thead> <tr> <th>Filesystem</th> <th>Size</th> <th>Used</th> <th>Avail</th> <th>Use%</th> <th>Mounted on</th> </tr> </thead> <tbody> <tr> <td>/dev/vdd</td> <td>2.0G</td> <td>69M</td> <td>2.3G</td> <td>1%</td> <td>/usr/opencv</td> </tr> </tbody> </table> | Filesystem | Size | Used | Avail | Use% | Mounted on | /dev/vdd | 2.0G | 69M | 2.3G | 1% | /usr/opencv | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Filesystem | Size | Used | Avail | Use% | Mounted on | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| /dev/vdd | 2.0G | 69M | 2.3G | 1% | /usr/opencv | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 126. Increase the PMAC NetBackup Files System Size

| Step | Procedure | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|---|---------|----|------|-------|------------------|----------|------------|--------|-------------------------|----------|------------|--------|-----------------------|----------|------------|--------|----------------------------|----------|------------|-------|-----------|--------|------------|---------|-----------|--------|------------|-------|----------|--------|------------|-------|----------|--------|------------|-------|----------|--------|------------|-------|
| <p>4. <input type="checkbox"/></p> | <p>TVOE Host: Resize volume</p> | <p>Resize the NetBackup volume from 2GB to 5GB.</p> <pre>[admusr@<tvoe_host> ~]\$ usr/bin/sudo /sbin/lvextend --size 5G /dev/vgguests/<pmac_guest>_netbackup.img</pre> <p>Size of logical volume vgguests/<pmac_guest>_netbackup.img changed from 2.00 GiB (64 extents) to 5.00 GiB (160 extents).</p> <p>Logical volume <pmac_guest>_netbackup.img successfully resized</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>5. <input type="checkbox"/></p> | <p>TVOE Host: Verify increase</p> | <p>Verify the size of the volume has increased to 5GB.</p> <p>1. Display the logical volume sizes.</p> <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /sbin/lvs</pre> <table border="1"> <thead> <tr> <th>LV</th> <th>VG</th> <th>Attr</th> <th>LSize</th> </tr> </thead> <tbody> <tr> <td><pmac_guest>.img</td> <td>vgguests</td> <td>-wi-ao----</td> <td>50.00g</td> </tr> <tr> <td><pmac_guest>_images.img</td> <td>vgguests</td> <td>-wi-ao----</td> <td>20.00g</td> </tr> <tr> <td><pmac_guest>_logs.img</td> <td>vgguests</td> <td>-wi-ao----</td> <td>10.00g</td> </tr> <tr style="background-color: yellow;"> <td><pmac_guest>_netbackup.img</td> <td>vgguests</td> <td>-wi-ao----</td> <td>5.00g</td> </tr> <tr> <td>plat_root</td> <td>vgroot</td> <td>-wi-ao----</td> <td>768.00m</td> </tr> <tr> <td>plat_swap</td> <td>vgroot</td> <td>-wi-ao----</td> <td>2.00g</td> </tr> <tr> <td>plat_tmp</td> <td>vgroot</td> <td>-wi-ao----</td> <td>1.00g</td> </tr> <tr> <td>plat_usr</td> <td>vgroot</td> <td>-wi-ao----</td> <td>3.00g</td> </tr> <tr> <td>plat_var</td> <td>vgroot</td> <td>-wi-ao----</td> <td>1.00g</td> </tr> </tbody> </table> <p>2. Display the logical volume details.</p> <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /sbin/lvdisplay /dev/vgguests/<pmac_guest>_netbackup.img</pre> <pre>--- Logical volume --- LV Path /dev/vgguests/<pmac_guest>_netbackup.img LV Name <pmac_guest>_netbackup.img VG Name vgguests LV UUID CWelNl-ln6r-22Tv-5B0p-Xj4F-44dM-SyGUwp LV Write Access read/write LV Creation host, time <tvoe_host>, 2016-11-14 10:00:54 -0500 LV Status available # open 1 LV Size 5.00 GiB Current LE 64 Segments 1 Allocation inherit Read ahead sectors auto - currently set to 4096 Block device 253:19</pre> | LV | VG | Attr | LSize | <pmac_guest>.img | vgguests | -wi-ao---- | 50.00g | <pmac_guest>_images.img | vgguests | -wi-ao---- | 20.00g | <pmac_guest>_logs.img | vgguests | -wi-ao---- | 10.00g | <pmac_guest>_netbackup.img | vgguests | -wi-ao---- | 5.00g | plat_root | vgroot | -wi-ao---- | 768.00m | plat_swap | vgroot | -wi-ao---- | 2.00g | plat_tmp | vgroot | -wi-ao---- | 1.00g | plat_usr | vgroot | -wi-ao---- | 3.00g | plat_var | vgroot | -wi-ao---- | 1.00g |
| LV | VG | Attr | LSize | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>.img | vgguests | -wi-ao---- | 50.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>_images.img | vgguests | -wi-ao---- | 20.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>_logs.img | vgguests | -wi-ao---- | 10.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <pmac_guest>_netbackup.img | vgguests | -wi-ao---- | 5.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_root | vgroot | -wi-ao---- | 768.00m | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_swap | vgroot | -wi-ao---- | 2.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_tmp | vgroot | -wi-ao---- | 1.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_usr | vgroot | -wi-ao---- | 3.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| plat_var | vgroot | -wi-ao---- | 1.00g | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 126. Increase the PMAC NetBackup Files System Size

| Step | Procedure | Results | | | | | | | | | | | | |
|--------------------------------|--|---|------------|------|-------------|-------|--------------|------------|----------|------|-------|------|--------------|-------------|
| 6. <input type="checkbox"/> | PMAC: Verify filesystem | <p>Verify the space on the PMAC NetBackup filesystem has not changed.</p> <pre>[admusr@<pmac_guest> ~]\$ /bin/df -h /usr/opencv</pre> <table border="1"> <thead> <tr> <th>Filesystem</th> <th>Size</th> <th>Used</th> <th>Avail</th> <th>Use%</th> <th>Mounted on</th> </tr> </thead> <tbody> <tr> <td>/dev/vdd</td> <td>2.0G</td> <td>69M</td> <td>2.3G</td> <td>1%</td> <td>/usr/opencv</td> </tr> </tbody> </table> | Filesystem | Size | Used | Avail | Use% | Mounted on | /dev/vdd | 2.0G | 69M | 2.3G | 1% | /usr/opencv |
| Filesystem | Size | Used | Avail | Use% | Mounted on | | | | | | | | | |
| /dev/vdd | 2.0G | 69M | 2.3G | 1% | /usr/opencv | | | | | | | | | |
| 7. <input type="checkbox"/> | TVOE Host: Verify PMAC is aware of volume size increase | <ol style="list-style-type: none"> Ensure the PMAC is made aware of the volume size increase. Identify the PMAC guest using the virsh command. <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /usr/bin/virsh list --all</pre> <table border="1"> <thead> <tr> <th>Id</th> <th>Name</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>86</td> <td><pmac_guest></td> <td>running</td> </tr> </tbody> </table> <p>Shut down the PMAC guest.</p> <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /usr/bin/virsh shutdown <pmac_guest></pre> <p>Domain <pmac_guest> is being shutdown</p> Wait for the PMAC shutdown to complete. If the State is running, repeat the command until it indicates the State is shut off. <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /usr/bin/virsh list --all</pre> <table border="1"> <thead> <tr> <th>Id</th> <th>Name</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>86</td> <td><pmac_guest></td> <td>shut off</td> </tr> </tbody> </table> Once shutdown is complete, restart the PMAC. <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /usr/bin/virsh start <pmac_guest></pre> <p>Domain <pmac_guest> started</p> Verify the PMAC has completed the restart. This can be checked by executing the command sudo virsh console <pmac_guest> and checking for the PMAC guest login prompt. <p>Once the escape character is displayed, press Enter once more to reach the login prompt.</p> <p>Afterwards, press Ctrl-] to exit the PMAC login prompt and return to the TVOE host prompt.</p> <pre>[admusr@<tvoe_host> ~]\$ /usr/bin/sudo /usr/bin/virsh console <pmac_guest></pre> <p>Connected to domain <tvoe_host></p> <p>Escape character is ^]</p> <p>Oracle Linux Server release 6.8</p> <p>Kernel 2.6.32-642.6.1.el6prere17.3.0.0.0_88.30.0.x86_64 on an x86_64</p> | Id | Name | State | 86 | <pmac_guest> | running | Id | Name | State | 86 | <pmac_guest> | shut off |
| Id | Name | State | | | | | | | | | | | | |
| 86 | <pmac_guest> | running | | | | | | | | | | | | |
| Id | Name | State | | | | | | | | | | | | |
| 86 | <pmac_guest> | shut off | | | | | | | | | | | | |

Procedure 126. Increase the PMAC NetBackup Files System Size

| Step | Procedure | Results |
|--|--|---|
| <p>8. <input type="checkbox"/></p> | <p>PMAC: Verify volume size</p> | <p>Verify the volume size increase is 5GB as seen from the PMAC.</p> <pre>[admusr@<pmac_guest> ~]\$ /usr/bin/sudo admusr /sbin/fdisk -l /dev/netbackup</pre> <p>Disk /dev/netbackup: 5368 MB, 5368709120 bytes 16 heads, 63 sectors/track, 10402 cylinders Units = cylinders of 1008 * 512 = 516096 bytes Sector size (logical/physical): 512 bytes / 512 bytes I/O size (minimum/optimal): 512 bytes / 512 bytes Disk identifier: 0x00000000</p> |
| <p>9. <input type="checkbox"/></p> | <p>PMAC: Resize filesystem</p> | <p>Resize the PMAC NetBackup filesystem to 5GB.</p> <ol style="list-style-type: none"> Verify the filesystem is still mounted by issuing the mount command and looking for /dev/vdd mounted on /usr/openv. <pre>[admusr@<pmac_guest> ~]\$ /bin/mount</pre> <pre>/dev/mapper/vgroot-plat_root on / type ext4 (rw)</pre> <pre>proc on /proc type proc (rw)</pre> <pre>sysfs on /sys type sysfs (rw)</pre> <pre>devpts on /dev/pts type devpts (rw,gid=5,mode=620)</pre> <pre>tmpfs on /dev/shm type tmpfs (rw)</pre> <pre>/dev/vda1 on /boot type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-plat_tmp on /tmp type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-plat_usr on /usr type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-plat_var on /var type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-plat_var_tklc on /var/TKLC type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-smac_root on /usr/TKLC/smac type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-smac_var on /var/TKLC/smac type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-smac_backup on /var/TKLC/smac/backup type ext4 (rw)</pre> <pre>/dev/mapper/vgroot-smac_isoimages on /var/TKLC/smac/image/isoimages type ext4 (rw)</pre> <pre>/var/TKLC/smac/image/core on /var/TKLC/core type none (rw,bind)</pre> <pre>/dev/vdb on /var/TKLC/smac/logs type ext3 (rw)</pre> <pre>/dev/vdc on /var/TKLC/smac/image/repository type ext3 (rw)</pre> <pre>none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)</pre> <pre>sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)</pre> <pre>nfsd on /proc/fs/nfsd type nfsd (rw)</pre> <pre>/dev/vdd on /usr/openv type ext3 (rw)</pre> Unmount the NetBackup filesystem. The umount command can be verified by issuing the mount command again. The /usr/openv filesystem should not be displayed as in the previous command. |

Procedure 126. Increase the PMAC NetBackup Files System Size

| Step | Procedure | Results |
|------|-----------|--|
| | | <p>Note: There umount command does not generate output upon success.</p> <pre>[admusr@<pmac_guest> ~]\$ /usr/bin/sudo /bin/umount /usr/opensv</pre> <p>3. Execute the e2fsck command to make sure the NetBackup filesystem is clean.</p> <pre>[admusr@<pmac_guest> ~]\$ /usr/bin/sudo /sbin/e2fsck /dev/netbackup e2fsck 1.43-WIP (20-Jun-2013) /dev/netbackup: clean, 11/327680 files, 37999/1310720 blocks</pre> <p>4. Execute the resize2fs command to resize the filesystem and map it to the 5GB size of the disk volume on the TVOE host. If the size attribute is not included in the command, the NetBackup filesystem resizes to the total free space on the TVOE host volume. This should be 5GB since there should not be any other filesystems mounted to this volume. If the resize2fs command returns an indication that the e2fsck command must be executed on the NetBackup filesystem, then re-execute that command.</p> <pre>[admusr@<pmac_guest> ~]\$ /usr/bin/sudo /usr/bin/resize2fs /dev/netbackup resize2fs 1.43-WIP (20-Jun-2013) Resizing the filesystem on /dev/netbackup to 1310720 (4k) blocks. The filesystem on /dev/netbackup is now 1310720 blocks long.</pre> <p>5. Re-mount the /usr/opensv NetBackup filesystem with the mount -a command.</p> <pre>[admusr@<pmac_guest> ~]\$ mount -a</pre> <p>Note: This command can only be used if the existing entry to mount the filesystem is contained in the /etc/fstab file (which is expected).</p> <p>6. Verify the new size of the NetBackup filesystem. Issue the mount command to verify the filesystem is correctly mounted. Issue the /bin/df -h /usr/opensv command to show the NetBackup filesystem using 5GB instead of 2GB.</p> <pre>[admusr@<pmac_guest> ~]\$ /bin/mount /dev/mapper/vgroot-plat_root on / type ext4 (rw) proc on /proc type proc (rw) sysfs on /sys type sysfs (rw) devpts on /dev/pts type devpts (rw,gid=5,mode=620) tmpfs on /dev/shm type tmpfs (rw) /dev/vdal on /boot type ext4 (rw) /dev/mapper/vgroot-plat_tmp on /tmp type ext4 (rw) /dev/mapper/vgroot-plat_usr on /usr type ext4 (rw) /dev/mapper/vgroot-plat_var on /var type ext4 (rw) /dev/mapper/vgroot-plat_var_tklc on /var/TKLC type ext4 (rw) /dev/mapper/vgroot-smac_root on /usr/TKLC/smac type ext4 (rw)</pre> |

Procedure 126. Increase the PMAC NetBackup Files System Size

| Step | Procedure | Results | | | | | | | | | | | | |
|------------|-----------|--|------------|------|------------|-------|------|------------|----------|------|-----|------|----|------------|
| | | <pre> /dev/mapper/vgroot-smac_var on /var/TKLC/smac type ext4 (rw) /dev/mapper/vgroot-smac_backup on /var/TKLC/smac/backup type ext4 (rw) /dev/mapper/vgroot-smac_isoimages on /var/TKLC/smac/image/isoimages type ext4 (rw) /var/TKLC/smac/image/core on /var/TKLC/core type none (rw,bind) /dev/vdb on /var/TKLC/smac/logs type ext3 (rw) /dev/vdc on /var/TKLC/smac/image/repository type ext3 (rw) none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw) sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw) nfsd on /proc/fs/nfsd type nfsd (rw) /dev/vdd on /usr/openv type ext3 (rw) </pre> <p>The second command in this sub-step shows the NetBackup filesystem using 5GB instead of 2GB.</p> <pre> [admusr@<pmac_guest> ~]\$ /bin/df -h /usr/openv </pre> <table border="1"> <thead> <tr> <th>Filesystem</th> <th>Size</th> <th>Used</th> <th>Avail</th> <th>Use%</th> <th>Mounted on</th> </tr> </thead> <tbody> <tr> <td>/dev/vdd</td> <td>5.0G</td> <td>69M</td> <td>4.3G</td> <td>1%</td> <td>/usr/openv</td> </tr> </tbody> </table> <p>7. Change the directory to the /usr/openv directory and verify any files contained on the original 2GB NetBackup filesystem are still available on the new 5GB NetBackup filesystem.</p> <pre> [admusr@<pmac_guest> ~]\$ /bin/ls -l /usr/openv </pre> <pre> java lost+found pack regid.1992-12.com.symantec_netbackup- 7.6.0.1_1.swidtag share var lib msg pack.7.6.0.1 regid.1992-12.com.symantec_netbackup- 7.7.1.0_1.swidtag swidtag.xml logs netbackup pdde resources tmp </pre> | Filesystem | Size | Used | Avail | Use% | Mounted on | /dev/vdd | 5.0G | 69M | 4.3G | 1% | /usr/openv |
| Filesystem | Size | Used | Avail | Use% | Mounted on | | | | | | | | | |
| /dev/vdd | 5.0G | 69M | 4.3G | 1% | /usr/openv | | | | | | | | | |

Appendix R. netConfig Backup Configuration/Restore Configuration/Upgrade Firmware with TPD Cipher Change

This procedure prepares the PMAC to avoid the cipher mismatch issue with Cisco switches. This is performed before the netConfig backup or restore operations.

Beginning with TPD 7.6.0.0_88.50.0, the cipher list is restricted to allow only a limited number of ciphers for ssh access to the servers. As a result, netConfig backup and restore operations are not functional with Cisco switches (3020, 4948s) since these switches use other ciphers. Executing these commands with the restricted ciphers would fail as shown here:

```

[admusr@p5-pmac ~]$ sudo netConfig --device=3020_ip backupConfiguration
service=ssh_ip filename=backup
Command failed: backupConfiguration
Error saving to SSH service
[admusr@p5-pmac ~]$

```

To avoid this issue while maintaining a focus on improved security, the Procedure 127 must be executed before and after netConfig backup and restore operations.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 127. Turn Off Cipher List Before Backup Configuration/Restore Configuration/Upgrade Firmware Command

| Step | Procedure | Results |
|--------------------------------|--|---|
| 1. <input type="checkbox"/> | Turn off cipher list | From the PMAC shell enter: <pre>sudo vi /etc/ssh/sshd_config</pre> Add # in the beginning of the following three lines to comment them out, the result is: <pre>#Ciphers aes256-ctr,aes192-ctr,aes128-ctr #MaxAuthTries 4 #LoginGraceTime 1m</pre> |
| 2. <input type="checkbox"/> | Restart sshd | <pre>sudo service sshd restart</pre> |
| 3. <input type="checkbox"/> | Run the netConfig backupConfiguration/restoreConfiguration/upgradeFirmware command | For a backup operation: <pre>[admusr@pmac ~]\$ sudo /usr/TKLC/plat/bin/netConfig backupConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup</pre> For a restore operation: <pre>[admusr@pmac ~]\$ sudo /usr/TKLC/plat/bin/netConfig restoreConfiguration --device=<switch_name> service=<ssh_service> filename=<switch_name>-backup</pre> For an upgrade operation: <pre>[admusr@pmac ~]\$ sudo /usr/TKLC/plat/bin/netConfig upgradeFirmware --device=<switch_name> service=<ssh_service> filename=<Cisco IOS></pre> |

This procedure restores the PMAC restricted cipher list after perform the netConfig backup and restore operations.

If a step fails to execute successfully, stop and contact **Error! Bookmark not defined.** for assistance.

Procedure 128. Resume Cipher List After Backup Configuration/Restore Configuration/Upgrade Firmware Command

| Step | Procedure | Results |
|--------------------------------|------------------------|---|
| 1. <input type="checkbox"/> | Resume the cipher list | From the PMAC shell enter: <pre>sudo vi /etc/ssh/sshd_config</pre> Uncomment the three lines: <pre>Ciphers aes256-ctr,aes192-ctr,aes128-ctr MaxAuthTries 4 LoginGraceTime 1m</pre> |
| 2. <input type="checkbox"/> | Restart sshd | <pre>sudo service sshd restart</pre> |

Appendix S. Enable SNMPv3 Support on the PMAC

This appendix provides the sub-procedures and steps required to enable overall SNMPv3 protocol support on the PMAC system.

There are multiple PMAC Procedures required to complete this appendix:

1. **Updating the SNMP service on existing remote servers on the PMAC control network.**

This sub-procedure is used to enable the SNMP service on the remote servers to support SNMPv3. It only applies to the servers (blades, guests, and RMS's) on the PMAC control network that have been fully discovered (both HW and SW).

It is important that the IPv6 address of each server be known first. The user is advised to create a list of hardware position vs. IPv6.

Once this sub-procedure is applied the servers changed will no longer be totally visible in the PMAC SW Inventory page. Possibly only the IPv6 is visible. Once the entire set of sub-procedures is complete, the remote servers will be totally SW discovered on the PMAC.

This sub-procedure can also be used to support the addition of a new server on the PMAC control network or to accommodate when an existing server is re-ipm'd. This must be followed because a newly IPM'd server will come into service supporting SNMPv2c and must be updated to support SNMPv3 if the PMAC has already had SNMPv3 enabled.

2. **Updating the SNMP service on the PMAC server service to support SNMPv3.**

This sub-procedure involves updating the PMAC server service to support SNMPv3. It is the same as sub-procedure 1 above only it applies to the PMAC itself.

3. **Updating the PMAC messaging system to support SNMPv3.**

This sub-procedure involves updating the PMAC messaging system to support SNMPv3. The messaging system does all the internal communication between the PMAC and the remote servers on the PMAC control network.

4. **Updating the SNMPv3 Security settings**

This sub-procedure is used when the customer wishes to change the current SNMPv3 default security settings. These settings can be changed at any time but it is recommended that this action be performed in a maintenance window. Also note that when these settings are changed, that same change must be reflected in every server that supports SNMPv3 on the PMAC control network (see sub-procedure 1).

The current default settings are as follows:

```
securityname : tklcpublic
authkey      : *****
privkey      : *****
authprotocol : SHA
privprotocol : AES
securitylevel : authPriv
context      : tklcpublic
```

Appendix S.1 Prerequisites

- PMAC is in-service and sentry is up and running.
- The PMAC currently supports SNMPv2c.
- Blades, guests and RMS servers are currently in-service, HW and SW discovered, and are supporting SNMPv2c (which is the default version of SNMP after deploy of any server on the PMAC control network).

Appendix S.2 Limitations

- Any remote servers on the PMAC control network not supporting the currently enabled protocol will be able to HW discover but will not be able to SW discover as shown in the SW Inventory page.
- The default setting for SNMP is SNMPv2c on PMAC deploy. Once the SNMP version is set to v3, it will be maintained on all upgrades.
- Once the SNMP version is set to SNMPv3, all servers previously SW discovered will no longer be “fully” SW discovered. The IPv6 may be visible in the address field of the Software Inventory page.
- Once SNMPv3 has been enabled on the PMAC, any newly IPM'd server must be changed to support SNMPv3 as per the instructions below.
- A remote server can be configured to support both SNMPv2c and SNMPv3. If that is the case, if the PMAC is returned to SNMPv2c, all servers on the control network that support both versions will SW discover correctly.
- If an existing server on the PMAC control network is re-ipm'd (or a new server is added to the control network), it will default to SNMPv2c. If the PMAC has been updated to support SNMPv3, the new server will not fully SW discover until it has been updated to support SNMPv3.

Appendix S.3 Procedural Notes:

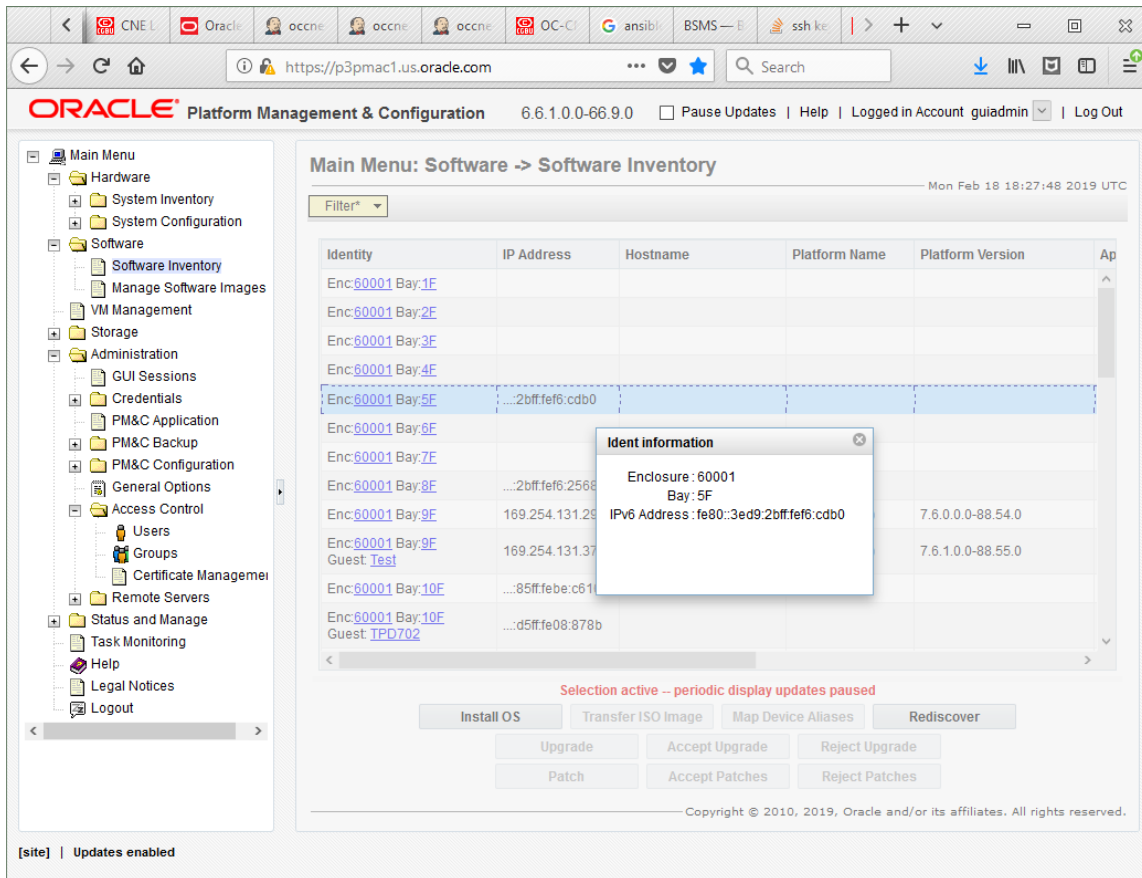
- The commands listed below require root access to execute them. `sudo` is used to elevate the user permissions to be able to execute the commands. Any command that is not prefixed with `sudo` does not require elevation to execute.
- All commands are executed from a PMAC shell or from a TVOE shell or from a remote server shell accessed via the PMAC shell using ssh.
- Each step in this procedure begins by identifying the target server on which the command is to be executed. In this procedure, commands are executed on either the PMAC, guest, blade or RMS.

Appendix S.4 Obtaining the IPv6 of a server (guest, blade, or RMS) on the control network of the PMAC

The IPv6 address of a server on the PMAC control network can be obtained in a number of ways. It depends on whether this server has been fully discovered or not.

1. Using the GUI:

The IPv6 will show up in the GUI at the **Main Menu->Software->Software Inventory** in a small dialog (or popup) when you double click the lpv6.



2. Using ntdMgr --show command:

The **ntdMgr --show** command display the list of known servers on the PMAC control network. This list includes the interface (control) the UUID and the IPv6. The command can be piped into **grep** to display just the value of the IPv6. The only issue is that it does not distinguish which server the IPv6 is associated with. If the last 4 digits of the IPv6 can be retrieved from the GUI (see above), then that 4 char string can be used in the grep command to get the full IPv6 address.

```
[root@p3Pmac1 ~]# /usr/TKLC/plat/bin/ntdMgr --show | grep control
fe80::3ed9:2bff:fe6:cdb0,control,20000,
fe80::a4:42ff:fe8f:4faa,control,20000,
fe80::dad3:85ff:febe:c610,control,20000,
fe80::3e4a:92ff:feed:6a30,control,20000,
fe80::2e76:8aff:fe50:7960,control,20000,
fe80::ed:d5ff:fe08:878b,control,20000,
fe80::9eb6:54ff:fe89:ed84,control,20000,
fe80::2e76:8aff:fe50:3974,control,20000,
fe80::9a4b:e1ff:fe68:1fd8,control,20000,
fe80::1ec1:deff:feed:8c38,control,20000,
fe80::1d:47ff:fe71:9b3,control,20000,
fe80::1ec1:deff:feed:9cd8,control,20000,
fe80::54:c3ff:fe43:14ba,control,20000,
```

3. Using the **ip -6 addr** command:

If the server has been fully discovered, the IPv6 can be obtained using the **ip -6 addr** command on the server. Look for the control interface to find the IPv6. Note that to get this info for a server on the PMAC control network, you must ssh `admusr@<server IPv4>` and use the default password.

```
[root@p3Pmac1 ~]# /sbin/ip -6 addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: control: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 fe80::5054:ff:fe1c:1ef0/64 scope link
        valid_lft forever preferred_lft forever
3: management: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 fe80::5054:ff:fe87:8c7e/64 scope link
        valid_lft forever preferred_lft forever
```

Appendix S.5 PMAC Procedures for Converting to SNMPv3

Procedure 129.Updating the SNMP Service on Existing Remote Servers on the PMAC Control Network

| Step | Procedure | Results |
|--------------------------------|------------------------------|--|
| 1. <input type="checkbox"/> | Log into the PMAC shell | Connect to the PMAC shell and log into the PMAC shell as admusr using ssh and the default admusr password. |
| 2. <input type="checkbox"/> | Connect to the remote server | <p>This step involves connecting to a remote server via the PMAC using SSH.</p> <p>Note: If this step involves setting the PMAC SNMP service to support SNMPv3, then there is no need to execute this step.</p> <ol style="list-style-type: none"> 1. Connect to the PMAC shell and log into the PMAC shell as admusr using ssh and the default password. 2. Note down the IPv6 address of the blade (see instructions above) 3. Log into the blade terminal as admusr using ssh from the PMAC shell by executing the below command. If the ipv4 address is known, the IPv4 address is preferable. <pre>/usr/bin/sudo /usr/bin/ssh admusr@<blade-ipv4-addr> or /usr/bin/sudo /usr/bin/ssh admusr@<blade-ipv6-addr>%control</pre> |

Procedure 129.Updating the SNMP Service on Existing Remote Servers on the PMAC Control Network

| Step | Procedure | Results |
|--------------------------------|---|--|
| 3. <input type="checkbox"/> | Enable SNMPv3 protocol on the remote server or PMAC | <p>1. Stop the SNMP service by executing the below command on blade terminal:</p> <pre>/usr/bin/sudo /sbin/stop TKLCSnmp</pre> <p>2. Configure the SNMP service to use SNMPv3 protocol by executing the below command on blade terminal:</p> <pre>/usr/bin/sudo /usr/bin/net-snmp-create-v3-user -ro -A <auth-key> -a <auth-protocol> -X <priv-key> -x <priv-protocol> <security-name></pre> <p>This adds the following line to /var/lib/net-snmp/snmpd.conf:</p> <pre>createUser tklcpublic <auth-protocol> <auth-key> <priv-protocol> <priv-key></pre> <p>And adds the following line to /etc/snmp/snmpd.conf:</p> <pre>rouser <security-name></pre> <p>Example:</p> <pre>/usr/bin/sudo /usr/bin/net-snmp-create-v3-user -ro -A tklcpublic -a SHA -X tklcpublic -x AES tklcpublic</pre> <p>Note: To use the SNMP service with security level set to “noAuthNoPriv”. It is required to manually edit the file “/etc/snmp/snmpd.conf” after executing the above command by adding the option “noauth” next to line “rouser <security-name>”.</p> <p>Example:</p> <pre>rouser <security-name> noauth</pre> <p>3. Restart the SNMP service by executing the below command on blade terminal.</p> <pre>/usr/bin/sudo /sbin/start TKLCSnmp</pre> <p>4. Check that the above configuration is successful by executing the following command and check that no error occurs.</p> <pre>/usr/bin/sudo /usr/bin/snmpwalk -u <security-name> -A <auth-key> -a <auth-protocol> -X <priv-key> -x <priv-protocol> -l <security-level> 127.0.0.1 -v3 TPD-CARD-CFG-MIB::tpdCardCfgPlatformSwVersion.0</pre> <p>Example:</p> <pre>/usr/bin/sudo /usr/bin/snmpwalk -u tklcpublic -A tklcpublic -a SHA -X tklcpublic -x DES -l authPriv 127.0.0.1 -v3 TPD-CARD-CFG-MIB::tpdCardCfgPlatformSwVersion.0</pre> |

Procedure 130.Update the SNMP Service on the PMAC Server to Support SNMPv3

| Step | Procedures | Results |
|--------------------------------|-------------------------------------|--|
| 1. <input type="checkbox"/> | Update the SNMP service on the PMAC | Execute Procedure 129 for the PMAC. Skip step 2 as per instructions. |

Procedure 131. Update the PMAC Messaging System to Support SNMPv3

| Step | Procedures | Results | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--------------------------------|--------------------------------------|--|------------|-----|--------|--|---------|------|--|--|-------|--|--|--|----------|------|---------|------------|-----------------|--|--|--|---------|------|---------|------------|-----------------|--|--|--|--------------|------|---------|------------|-----------------|--|--|--|------------------|------|---------|------------|-----------------|--|--|--|
| 1. <input type="checkbox"/> | Login to the PMAC shell | Connect to the PMAC shell and log into the PMAC shell as admusr using ssh. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2. <input type="checkbox"/> | Update the snmpVersion parameter | <ol style="list-style-type: none"> 1. On deploy or upgrade of the PMAC, the default value of parameter 'snmpVersion' in the table 'ConfigDB.params' is set to 'snmpv2c'. 2. Set the parameter 'snmpVersion' to 'snmpv3' by executing the following command on PMAC terminal: <pre data-bbox="623 569 1263 653">/usr/bin/sudo /usr/TKLC/smac/bin/pmacadm setParam --paramName=snmpVersion -- paramValue=snmpv3</pre> 3. Verify the current value of the parameter 'snmpVersion' is 'snmpv3' by executing the below command: <pre data-bbox="623 741 1263 800">/usr/bin/sudo /usr/TKLC/smac/bin/pmacadm getParam --paramName=snmpVersion</pre> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3. <input type="checkbox"/> | Perform a sentry restart on the PMAC | <ol style="list-style-type: none"> 1. Perform a sentry restart. <pre data-bbox="623 863 1373 890">/usr/bin/sudo /usr/TKLC/smac/bin/sentry restart</pre> 2. Check the sentry has been restart by executing the below command. Keep executing the command until all the processes are running like the example below. <pre data-bbox="578 1010 1308 1037">/usr/bin/sudo /usr/TKLC/smac/bin/sentry status</pre> <p data-bbox="578 1087 971 1115">sending status command...</p> <p data-bbox="578 1125 862 1152">PM&C Sentry Status</p> <p data-bbox="578 1163 862 1190">-----</p> <p data-bbox="578 1201 1230 1228">sentryd started: Mon Feb 18 04:45:05 2019</p> <p data-bbox="578 1239 1040 1266">Current activity mode: ACTIVE</p> <table border="1" data-bbox="578 1276 1386 1640"> <thead> <tr> <th>Process</th> <th>PID</th> <th>Status</th> <th></th> </tr> <tr> <th>StartTS</th> <th>NumR</th> <th></th> <th></th> </tr> <tr> <th colspan="4">-----</th> </tr> </thead> <tbody> <tr> <td>smacTalk</td> <td>8910</td> <td>running</td> <td>Mon Feb 18</td> </tr> <tr> <td>04:45:05 2019 1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>smacMon</td> <td>8935</td> <td>running</td> <td>Mon Feb 18</td> </tr> <tr> <td>04:45:05 2019 1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>hpiPortAudit</td> <td>8960</td> <td>running</td> <td>Mon Feb 18</td> </tr> <tr> <td>04:45:05 2019 1</td> <td></td> <td></td> <td></td> </tr> <tr> <td>snmpEventHandler</td> <td>8987</td> <td>running</td> <td>Mon Feb 18</td> </tr> <tr> <td>04:45:05 2019 1</td> <td></td> <td></td> <td></td> </tr> </tbody> </table> <p data-bbox="578 1692 959 1719">Mon Feb 18 04:46:53 2019</p> <p data-bbox="578 1730 846 1757">Command Complete.</p> | Process | PID | Status | | StartTS | NumR | | | ----- | | | | smacTalk | 8910 | running | Mon Feb 18 | 04:45:05 2019 1 | | | | smacMon | 8935 | running | Mon Feb 18 | 04:45:05 2019 1 | | | | hpiPortAudit | 8960 | running | Mon Feb 18 | 04:45:05 2019 1 | | | | snmpEventHandler | 8987 | running | Mon Feb 18 | 04:45:05 2019 1 | | | |
| Process | PID | Status | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| StartTS | NumR | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ----- | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| smacTalk | 8910 | running | Mon Feb 18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 04:45:05 2019 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| smacMon | 8935 | running | Mon Feb 18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 04:45:05 2019 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| hpiPortAudit | 8960 | running | Mon Feb 18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 04:45:05 2019 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| snmpEventHandler | 8987 | running | Mon Feb 18 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 04:45:05 2019 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Procedure 132. Setting the PMAC security Levels

| Step | Procedures | Results |
|--------------------------------|---------------------------------------|--|
| 1. <input type="checkbox"/> | Login to the PMAC shell | Connect to the PMAC shell and log into the PMAC shell as admusr using ssh. |
| 2. <input type="checkbox"/> | Update SNMP service on remote servers | Ensure all remote servers SNMP service has been updated to reflect the new security settings by executing sub-procedure1. |
| 3. <input type="checkbox"/> | Update SNMP service on the PMAC | Ensure the PMAC SNMP service has been updated to reflect the new security settings by executing sub-procedure 1 for PMAC. |
| 4. <input type="checkbox"/> | Configure SNMPv3 Security Settings | <p>1. Configure the SNMPv3 security settings in PMAC by executing the below command and enter the appropriate details when prompted:</p> <p>Note: The auth and priv key values are echoed as “*”. Care must be taken when entering these values to insure correctness.</p> <pre> /usr/bin/sudo /usr/TKLC/smac/bin/pmacadm updSnmPV3Security Enter Security Name: tklcpublic Enter auth key (minimum 8 chars): ***** Enter priv key (minimum 8 chars): ***** Enter Auth Protocol <MD5, SHA> : SHA Enter Priv Protocol <AES, DES> : AES Enter Security Level <noAuthNoPriv, authNoPriv, authPriv> : authPriv Enter Context: tklcpublic </pre> <p>2. Check that the SNMPv3 security settings in PMAC are correctly set by executing the below command:</p> <pre> /usr/bin/sudo usr/TKLC/smac/bin/pmacadm getSnmPV3Security securityname : tklcpublic authkey : ***** privkey : ***** authprotocol : SHA privprotocol : AES securitylevel : authPriv context : tklcpublic </pre> |

Procedure 132. Setting the PMAC security Levels

| Step | Procedures | Results |
|--------------------------------|-------------------------------------|---|
| 5. <input type="checkbox"/> | Perform a sentry restart | <ol style="list-style-type: none"> Restart the sentry by executing the below command on the PMAC terminal: <code>/usr/bin/sudo /usr/TKLC/smac/bin/sentry restart</code> Check that sentry has been restart by executing the below command. Keep executing the command until all the processes are running like the example below. <code>/usr/bin/sudo /usr/TKLC/smac/bin/sentry status</code> <pre> sending status command... PM&C Sentry Status ----- sentryd started: Mon Feb 18 04:45:05 2019 Current activity mode: ACTIVE Process PID Status StartTS NumR ----- smacTalk 8910 running Mon Feb 18 04:45:05 2019 1 smacMon 8935 running Mon Feb 18 04:45:05 2019 1 hpiPortAudit 8960 running Mon Feb 18 04:45:05 2019 1 snmpEventHandler 8987 running Mon Feb 18 04:45:05 2019 1 Mon Feb 18 04:46:53 2019 Command Complete. </pre> |
| 6. <input type="checkbox"/> | Ensure Software Discovery completes | <ol style="list-style-type: none"> Login to PMAC GUI. Navigate to Software > Software Inventory and make sure software discovery is successful. This may take some time depending on the number of servers on the PMAC control network. |

Appendix T. My Oracle Support (MOS)

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

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

- Select **2** for New Service Request.
- Select **3** for Hardware, Networking and Solaris Operating System Support.
- Select one of the following options:
 - For technical issues such as creating a new Service Request (SR), select 1.
 - For non-technical issues such as registration or assistance with MOS, select 2.

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

Emergency Response

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

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

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

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

Locate Product Documentation on the Oracle Help Center

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

1. Access the **Oracle Help Center** site at <http://docs.oracle.com>.
2. Click Industries.
3. Under the **Oracle Communications** subheading, click the **Oracle Communications documentation** link. The Communications Documentation page appears. Most products covered by these documentation sets display under the headings **Network Session Delivery and Control Infrastructure** or **Platforms**.
4. Click on your Product and then the Release Number. A list of the entire documentation set for the selected product and release displays. To download a file to your location, right-click the PDF link, select **Save target as** (or similar command based on your browser), and save to a local folder.