Oracle Communications Diameter Signaling Router Cloud Installation Guide, Release 8.0/8.1

Copyright © 2017 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 http://www.oracle.com/us/support/contact/index.html.

See more information on My Oracle Support (MOS) in Appendix I.
Table of Contents

1. Introduction .............................................................................................................................. 7
   1.1 Purpose and Scope ............................................................................................................. 7
   1.2 References ....................................................................................................................... 7
   1.3 Acronyms ......................................................................................................................... 8
   1.4 Terminology .................................................................................................................... 9

2. General Description ................................................................................................................ 10

3. Installation Overview .............................................................................................................. 11
   3.1 Required Materials ........................................................................................................... 11
   3.2 Installation Overview ...................................................................................................... 11
      3.2.1 Installation Strategy ................................................................................................. 11
      3.2.2 SNMP Configuration ............................................................................................... 12
      3.2.3 Installation Procedures ............................................................................................ 13
   3.3 Optional Features ............................................................................................................. 14

4. Software Installation Procedure ............................................................................................ 15
   4.1 Create DSR Guests (VMware) ............................................................................................ 16
   4.2 Create DSR Guests (KVM/OpenStack) ............................................................................. 18
   4.3 Create DSR Guests (OVM-S/OVM-M) ............................................................................. 24
   4.4 Configure Virtual Machines ............................................................................................ 28
   4.5 Application Configuration ............................................................................................... 36
   4.6 Configure Signaling Devices (Optional) ............................................................................ 97
   4.7 Configure Signaling Network Routes .............................................................................. 99
   4.8 Configure DSCP (Optional) ............................................................................................ 103
   4.9 Configure IP Front End (Optional) ............................................................................... 106
   4.10 SNMP Configuration (Optional) .................................................................................. 111
   4.11 Create iDIH Virtual Machines - VMware (Optional) .................................................... 112
   4.12 Create iDIH Virtual Machines - KVM/OpenStack (Optional) ........................................ 114
   4.13 Create iDIH Virtual Machines - OVM-S/OVM-M (Optional) ........................................ 118
   4.14 Configure iDIH Virtual Machines (Optional) ............................................................... 126
   4.15 Post iDIH Installation Configuration (Optional) ............................................................ 129
   4.16 Post-Install Activities .................................................................................................... 145

Appendix A. Sample Network Element and Hardware Profiles .............................................. 158

Appendix B. List of Frequently Used Time Zones ................................................................. 158

Appendix C. Common KVM/OpenStack Tasks ................................................................. 161
   Appendix C.1 Create a Network Port .................................................................................. 161
   Appendix C.2 Create and Boot OpenStack Instance ......................................................... 162
   Appendix C.3 Configure Networking for OpenStack Instance ........................................ 163
Appendix D. Common OVM Manager Tasks (CLI) ................................................................. 163
Appendix D.1 Setting Up the Server .................................................................................. 163
Appendix D.2 Server Pool ................................................................................................. 169

Appendix E. Firewall Ports ............................................................................................... 170

Appendix F. Application VIP Failover Options (OpenStack) ............................................. 170
Appendix F.1 Application VIP Failover Options ............................................................... 170
Appendix F.2 Allowed Address Pairs ................................................................................ 172
Appendix F.3 OpenStack Configuration Requirements .................................................... 172
Appendix F.4 After a VM Instance has been Booted: Allowed Address Pairs ................. 173
Appendix F.5 Before a VM Instance has been Booted: Allowed Address Pairs ............... 173
Appendix F.6 Disable Port Security .................................................................................. 174
Appendix F.7 After a VM Instance has been Booted: Port Security ................................ 175
Appendix F.8 Before a VM Instance has been Booted: Port Security ............................. 175
Appendix F.9 Managing Application Virtual IP Addresses within VM Instances .............. 176

Appendix G. Sample Net Rules File ................................................................................... 176

Appendix H. Performance Tuning Recommended ............................................................ 177
Appendix H.1 KVM/OpenStack ......................................................................................... 177
Appendix H.2 VMware ..................................................................................................... 178

Appendix I. My Oracle Support (MOS) ............................................................................ 179

List of Tables
Table 1. Acronyms ............................................................................................................. 8
Table 2. Terminology ......................................................................................................... 9
Table 3. Installation Overview ......................................................................................... 13
Table 4. Post-DSR Installation Configuration Step .......................................................... 14
Table 5. List of Selected Time Zone Values ...................................................................... 159

List of Figures
Figure 1. Initial Application Installation Path – Example shown ....................................... 10
Figure 2. DSR Single Site Installation Procedure Map .................................................... 12
Figure 3. Example Network Element XML File ............................................................... 158
Figure 4. Neutron High-Level Data Model ...................................................................... 171

List of Procedures
Procedure 1. (VMware) Import DSR OVA ................................................................. 16
Procedure 2. (VMware only) Configure NOAM Guests Role Based On Resource Profile and Configure Network ................................................................. 16
Procedure 3. (VMware only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network .......................................................... 17
Procedure 4. Import DSR OVA (KVM/OpenStack Only) .......................................................... 18
Procedure 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile ....... 19
Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network .......................................................... 21
Procedure 8. (OVM-S/OVM-M). Configure each DSR VM .......................................................... 28
Procedure 9. Configure the First NOAM NE and Server .......................................................... 36
Procedure 10. Configure the NOAM Server Group ........................................................................ 41
Procedure 11. Configure the Second NOAM Server ....................................................................... 45
Procedure 12. Complete Configuring the NOAM Server Group ....................................................... 48
Procedure 13. Configure the DR NOAM NE and Server (Optional) .................................................. 51
Procedure 14. Configure the DR NOAM Server Group (Optional) ................................................... 55
Procedure 15. Configure the Second DR NOAM Server (Optional) ................................................... 58
Procedure 16. Complete Configuring the DR NOAM Server Group (Optional) ................................. 62
Procedure 17. Configure the SOAM NE ....................................................................................... 65
Procedure 18. Configure the SOAM Servers .................................................................................. 67
Procedure 19. Configure the SOAM Server Group ........................................................................ 71
Procedure 20. Activate PCA/DCA (PCA/DCA Only) ...................................................................... 75
Procedure 21. Configure the MP Virtual Machines ........................................................................ 75
Procedure 22. Configure the MP Virtual Machines (Optional) ........................................................... 84
Procedure 23. Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only) .... 90
Procedure 24. Configure the MP Server Group(s) and Profiles ......................................................... 91
Procedure 25. Configure the Signaling Devices (Optional) ............................................................. 97
Procedure 26. Configure the Signaling Network Routes ................................................................... 99
Procedure 27. Configure DSCP Values for Outgoing Traffic (Optional) ............................................ 103
Procedure 28. IP Front End (IPFE) Configuration .......................................................................... 106
Procedure 29. Configure SNMP Trap Receiver(s) (Optional) ........................................................... 111
Procedure 30. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional) ........ 112
Procedure 31. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional) ................................................................................................. 114
Procedure 32. (OVM-S/OVM-M). Import Three iDIH OVAs and Create and Configure a VM for each ... 118
Procedure 33. Configure iDIH VM Networks (Optional) ................................................................... 126
Procedure 34. Run Post Installation Scripts on iDIH VMs (Optional) ................................................ 129
Procedure 35. Configure DSR Reference Data Synchronization for iDIH (Optional) ......................... 131
Procedure 36. iDIH Configuration: Configuring the SSO Domain (Optional) ..................................... 134
Procedure 37. Integrate iDIH into DSR (Optional) .......................................................................... 140
Procedure 38. iDIH Configuration: Configure the Mail Server (Optional) ........................................ 141
Procedure 39. iDIH Configuration: Configure SNMP Management Server (Optional) .................... 143
Procedure 40. iDIH Configuration: Change Network Interface (Optional) ......................................... 144
Procedure 41. Configure ComAgent Connections ........................................................................... 145
Procedure 42. Complete PCA Configuration (Optional) ................................................................. 152
Procedure 43. Backups and Disaster Prevention ............................................................................. 152
Procedure 44. (KVM/OpenStack Only) Configure Port Security ...................................................... 156
Procedure 45. Enable/Disable DTLS (SCTP Diameter Connections Only) ........................................ 157
Procedure 46. Shared Secret Encryption Key Revocation (RADIUS Only) ..................................... 157
Procedure 47. DSR Performance Tuning ........................................................................................... 157
1. Introduction

1.1 Purpose and Scope
This document describes the application-related installation procedures for Diameter Signaling Router Cloud system.
This document assumes platform-related configuration has already been done.
The audience for this document includes Oracle customers as well as these groups: Software System, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application.

1.2 References
[4] DSR Full Address Based Resolution (FABR) Feature Activation Procedure
[5] DSR Range Based Address Resolution (RBAR) Feature Activation
[7] MAP-Diameter IWF Feature Activation Procedure
[12] Range Based Address Resolution (RBAR) User’s Guide
[15] DSR Alarms and KPIs Reference
[16] Measurements Reference
[21] DSR IPv6 Migration Guide
[22] DSR DTLS Feature Activation Procedure
[23] DSR RADIUS Shared Secret Encryption Key Revocation MOP MO008572
[26] Networking v2.0 API documentation
[27] DSR Cloud Benchmarking Guide
1.3 Acronyms

An alphabetized list of acronyms used in the document.

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD</td>
<td>Compact Disk</td>
</tr>
<tr>
<td>DA-MP</td>
<td>Diameter Agent Message Processor</td>
</tr>
<tr>
<td>DSCP</td>
<td>Differentiated Services Code Point</td>
</tr>
<tr>
<td>DSR</td>
<td>Diameter Signaling Router</td>
</tr>
<tr>
<td>ESXi</td>
<td>Elastic Sky X Integrated</td>
</tr>
<tr>
<td>FABR</td>
<td>Full Address Based Resolution</td>
</tr>
<tr>
<td>iDIH</td>
<td>Integrated Diameter Intelligence Hub</td>
</tr>
<tr>
<td>IPFE</td>
<td>IP Front End</td>
</tr>
<tr>
<td>IWF</td>
<td>Inter Working Function</td>
</tr>
<tr>
<td>KVM</td>
<td>Kernel-based Virtual Machine</td>
</tr>
<tr>
<td>MP</td>
<td>Message Processor</td>
</tr>
<tr>
<td>NAPD</td>
<td>Network Architecture Planning Diagram</td>
</tr>
<tr>
<td>NE</td>
<td>Network Element</td>
</tr>
<tr>
<td>NOAM</td>
<td>Network Operation Administration and Maintenance</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System (e.g. TPD)</td>
</tr>
<tr>
<td>OVA</td>
<td>Open Virtualization Archive</td>
</tr>
<tr>
<td>OVM-M</td>
<td>Oracle VM Manager</td>
</tr>
<tr>
<td>OVM-S</td>
<td>Oracle VM Server</td>
</tr>
<tr>
<td>PDRA</td>
<td>Policy Diameter Routing Agent</td>
</tr>
<tr>
<td>PCA</td>
<td>Policy and Charging Application</td>
</tr>
<tr>
<td>RBAR</td>
<td>Range Based Address Resolution</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage Area Network</td>
</tr>
<tr>
<td>SFTP</td>
<td>Secure File Transfer Protocol</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SOAM</td>
<td>Software Operation Administration and Maintenance</td>
</tr>
<tr>
<td>SSO</td>
<td>Single Sign On</td>
</tr>
<tr>
<td>TPD</td>
<td>Tekelec Platform Distribution</td>
</tr>
<tr>
<td>TSA</td>
<td>Target Set Address</td>
</tr>
<tr>
<td>VIP</td>
<td>Virtual IP</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>vSTP</td>
<td>Virtual Signaling Transfer Point</td>
</tr>
</tbody>
</table>
1.4 Terminology

Multiple server types may be involved with the procedures in this manual. Therefore, most steps in the written procedures begin with the name or type of server to which the step applies.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Site                                      | Applicable for various applications, a site is type of “place”. A place is configured object that allows servers to be associated with a physical location.  
A site place allows servers to be associated with a physical site. For example, sites may be configured for Atlanta, Charlotte, and Chicago. Every server is associated with exactly one site when the server is configured.  
For the Policy & Charging DRA application, when configuring a site, only put DA-MPs and SBR MP servers in the site. Do not add NOAM, SOAM, or IPFE MPs to a site. |
| Place Association                         | Applicable for various applications, a “Place Association” is a configured object that allows places to be grouped together. A place can be a member of more than one place association.  
The Policy & Charging DRA application defines two place association types: policy binding region and policy & charging mated sites. |
| Policy & Charging SBR Server Group Redundancy | The Policy and Charging application uses SBR server groups to store the application data. The SBR server groups support both two and three site redundancy. The server group function name is “Policy & Charging SBR.” |
| Server Group Primary Site                 | A server group primary site is a term used to represent the principle location within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several sites (places).  
For the Policy & Charging DRA application, these sites (places) are all configured within a single “Policy and Charging Mated Sites” place association.  
The primary site may be in a different site (place) for each configured SOAM or SBR server group.  
A primary site is described as the location in which the active and standby servers to reside; however, there cannot be any preferred spare servers within this location.  
All SOAM and SBR server groups have a primary site. |
| Server Group Secondary Site               | A server group secondary site is a term used to represent location in addition to the Primary Site within a SOAM or SBR Server Group. SOAM and SBR server groups are intended to span several sites (places).  
For the Policy & Charging DRA application, these sites (places) are all configured within a single “Policy and Charging Mated Sites” place association.  
The secondary site may be in a different sites (places) for each configured SOAM or SBR server group.  
A secondary site is described as the location in which only preferred spare servers reside. The active and standby servers cannot reside within this location. If two site redundancy is wanted, a secondary site is required for all SOAM and SBR server groups. |
### Term | Definition
--- | ---
Session Binding Repository Server Group Redundancy | The DCA application may use SBR server groups to store application session data. The SBR server groups support both two and three site redundancy. The server group function name is “Session and Binding Repository.”
Two Site Redundancy | Two site redundancy is a data durability configuration in which Policy and Charging data is unaffected by the loss of one site in a Policy & Charging Mated Sites Place Association containing two sites. Two site redundancy is a feature provided by server group configuration. This feature provides geographic redundancy. Some server groups can be configured with servers located in two geographically separate sites (locations). This feature ensures there is always a functioning active server in a server group even if all the servers in a single site fail.

### 2. General Description

This document defines the steps to execute the initial installation of the Diameter Signaling Router (DSR) 8.0/8.1 application on a supported Cloud platform.

DSR installation paths are shown in the figures below. The general timeline for all processes to perform a software installation/configuration and upgrade is also included below.

This document covers initial installation of the DSR X.X.X application on a Cloud system.

![Diagram](image-url)

**Figure 1. Initial Application Installation Path – Example shown**
3. Installation Overview

This section provides a brief overview of the recommended method for installing the source release software that is installed and running on a Cloud to the target release software. The basic installation process and approximate time required is outlined in Table 2.

3.1 Required Materials

1. One target release DSR OVA Media
2. Three (3) iDIH Mediation OVA (Optional iDIH)
   a. iDIH Application OVA
   b. iDIH Oracle OVA
   c. iDIH Mediation OVA

3.2 Installation Overview

This section describes the overall strategy to employ for a single or multi-site DSR and iDIH installation. It also lists the procedures required for installation with estimated times. Section 3.2.1 discusses the overall installation strategy and includes an installation flowchart to determine exactly which procedures should be run for an installation. Section 3.2.3 lists the steps required to install a DSR system. The later sections expand on the information from the matrix and provide a general timeline for the installation. Additionally, basic firewall port information is included Appendix E Firewall Ports. It should also be noted that some procedures are cloud platform dependent and not all procedures are performed on all cloud platforms.

3.2.1 Installation Strategy

A successful installation of DSR requires careful planning and assessment of all configuration materials and installation variables.

Figure 2. DSR Single Site Installation Procedure Map illustrates the overall process that each DSR installation involves. In summary:

1. An overall installation requirement is decided upon. Among the data that should be collected:
   - The total number of sites
   - The number of virtual machines at each site and their role(s)
   - What time zone should be used across the entire collection of DSR sites?
   - Will SNMP traps be viewed at the NOAM or will an external NMS be used? (Or both?)
2. A site survey (NAPD) is conducted with the customer to determine exact networking and site details.

*Note:* XMI and IMI addresses are difficult to change once configured. It is **very important these addresses are well planned and not expected to change after a site is installed.**
3.2.2 SNMP Configuration

The network-wide plan for SNMP configuration should be decided upon before DSR installation proceeds. This section provides some recommendations for these decisions.

SNMP traps can originate from DSR Application Servers (NOAM, SOAM, MPs of all types) in a DSR installation.

DSR application servers can be configured to:

1. Send all their SNMP traps to the NOAM via merging from their local SOAM. All traps terminate at the NOAM and are viewable from the NOAM GUI (entire network) and the SOAM GUI (site specific). Traps are displayed on the GUI both as alarms and logged in trap history. **This is the default configuration option and no changes are required for this to take effect.**

2. Send all their SNMP traps to an external Network Management Station (NMS). The traps are seen at the SOAM and/or NOAM as alarms **AND** they are viewable at the configured NMS(s) as traps.
Application server SNMP configuration is done from the NOAM GUI near the end of DSR installation. See the procedure list for details.

### 3.2.3 Installation Procedures

The following table illustrates the progression of the installation process by procedure with estimated times. The estimated times and the phases that must be completed may vary due to differences in typing ability and system configuration. The phases outlined in are to be executed in the order they are listed.

#### Table 3. Installation Overview

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Phase</th>
<th>Elapsed Time (Minutes)</th>
<th>This Step</th>
<th>Cum.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure 1 or 4 or 7</td>
<td>Import DSR OVA</td>
<td>5</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Procedure 2 or 5</td>
<td>Configure DSR NOAM guest role based on resource profile</td>
<td>10</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Procedure 3 or 6</td>
<td>Configure DSR remaining guests role based on resource profile</td>
<td>40</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>Procedure 9</td>
<td>Configure the First NOAM NE and Server</td>
<td>25</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>Procedure 10</td>
<td>Configure the NOAM Server Group</td>
<td>15</td>
<td>95</td>
<td></td>
</tr>
<tr>
<td>Procedure 11</td>
<td>Configure the Second NOAM Server</td>
<td>15</td>
<td>110</td>
<td></td>
</tr>
<tr>
<td>Procedure 12</td>
<td>Complete Configuring the NOAM Server Group</td>
<td>10</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>Procedure 13 (Optional)</td>
<td>Configure the DR NOAM NE and Server (Optional)</td>
<td>25</td>
<td>145</td>
<td></td>
</tr>
<tr>
<td>Procedure 14 (Optional)</td>
<td>Configure the DR NOAM Server Group (Optional)</td>
<td>15</td>
<td>160</td>
<td></td>
</tr>
<tr>
<td>Procedure 15 (Optional)</td>
<td>Configure the Second DR NOAM Server (Optional)</td>
<td>15</td>
<td>175</td>
<td></td>
</tr>
<tr>
<td>Procedure 16 (Optional)</td>
<td>Complete Configuring the DR NOAM Server Group (Optional)</td>
<td>10</td>
<td>185</td>
<td></td>
</tr>
<tr>
<td>Procedure 17</td>
<td>Configure the SOAM NE</td>
<td>15</td>
<td>200</td>
<td></td>
</tr>
<tr>
<td>Procedure 18</td>
<td>Configure the SOAM Servers</td>
<td>10</td>
<td>210</td>
<td></td>
</tr>
<tr>
<td>Procedure 19</td>
<td>Configure the SOAM Server Group</td>
<td>10</td>
<td>220</td>
<td></td>
</tr>
<tr>
<td>Procedure 20</td>
<td>Activate PCA/DCA (PCA/DCA Only)</td>
<td>10</td>
<td>230</td>
<td></td>
</tr>
<tr>
<td>Procedure 21</td>
<td>Configure the MP Virtual Machines</td>
<td>5</td>
<td>235</td>
<td></td>
</tr>
<tr>
<td>Procedure 22 (Optional)</td>
<td>Configure the MP Virtual Machines (Optional)</td>
<td>10</td>
<td>245</td>
<td></td>
</tr>
<tr>
<td>Procedure 23</td>
<td>Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only)</td>
<td>10</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>Procedure 24</td>
<td>Configure the MP Server Group(s) and Profiles</td>
<td>5</td>
<td>260</td>
<td></td>
</tr>
<tr>
<td>Procedure 25 (Optional)</td>
<td>Configure the Signaling Devices (Optional)</td>
<td>10</td>
<td>270</td>
<td></td>
</tr>
<tr>
<td>Procedure 26</td>
<td>Configure the Signaling Network Routes</td>
<td>20</td>
<td>290</td>
<td></td>
</tr>
<tr>
<td>Procedure 27 (Optional)</td>
<td>Configure DSCP Values for Outgoing Traffic (Optional)</td>
<td>5</td>
<td>295</td>
<td></td>
</tr>
<tr>
<td>Procedure 28</td>
<td>IP Front End (IPFE) Configuration</td>
<td>45</td>
<td>340</td>
<td></td>
</tr>
<tr>
<td>Procedure 29 (Optional)</td>
<td>Configure SNMP Trap Receiver(s) (Optional)</td>
<td>15</td>
<td>355</td>
<td></td>
</tr>
<tr>
<td>Procedure</td>
<td>Phase</td>
<td>Elapsed Time (Minutes)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-------</td>
<td>------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 30</td>
<td>(VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)</td>
<td>10 365</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 31</td>
<td>(KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)</td>
<td>10 375</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 32</td>
<td>(OVM-S/OVM-M). Import Three IDIH OVs and Create and Configure a VM for each</td>
<td>10 385</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 33 (Optional)</td>
<td>Configure IDIH VM Networks (Optional)</td>
<td>10 395</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 34 (Optional)</td>
<td>Run Post Installation Scripts on IDIH VMs (Optional)</td>
<td>25 420</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 35 (Optional)</td>
<td>Configure DSR Reference Data Synchronization for IDIH (Optional)</td>
<td>30 450</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 36 (Optional)</td>
<td>iDIH Configuration: Configuring the SSO Domain (Optional)</td>
<td>10 460</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 37 (Optional)</td>
<td>Integrate IDIH into DSR (Optional)</td>
<td>10 470</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 38 (Optional)</td>
<td>iDIH Configuration: Configure the Mail Server (Optional)</td>
<td>10 480</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 39</td>
<td>iDIH Configuration: Configure SNMP Management Server (Optional)</td>
<td>20 500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 40 (Optional)</td>
<td>iDIH Configuration: Change Network Interface (Optional)</td>
<td>30 530</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 41</td>
<td>Configure ComAgent Connections</td>
<td>15 545</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 42</td>
<td>Complete PCA Configuration (Optional)</td>
<td>5 550</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 43</td>
<td>Backups and Disaster Prevention</td>
<td>15 565</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 44 (KVM/OpenStack Only)</td>
<td>Configure Port Security</td>
<td>10 575</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 46</td>
<td>Enable/Disable DTLS (SCTP Diameter Connections Only)</td>
<td>10 585</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 46</td>
<td>Shared Secret Encryption Key Revocation (RADIUS Only)</td>
<td>10 595</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procedure 47</td>
<td>DSR Performance Tuning</td>
<td>10 600</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.3 Optional Features

When DSR installation is complete, further configuration and/or installation steps are needed for optional features that may be present in this deployment. Please refer to Table 4 for the post-DSR installation configuration documentation needed for their components.

**Table 4. Post-DSR Installation Configuration Step**

| Feature                          | Document                                                        |
|---------------------------------|                                                                |
| Diameter Mediation              | DSR Meta Administration Feature Activation Procedure            |
| Full Address Based Resolution (FABR) | DSR FABR Feature Activation Procedure                          |
### Feature Document

<table>
<thead>
<tr>
<th>Feature</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>Range Based Address Resolution (RBAR)</td>
<td>DSR RBAR Feature Activation, Procedure</td>
</tr>
<tr>
<td>MAP-Diameter Interworking (MAP-IWF)</td>
<td>DSR MAP-Diameter IWF Feature Activation</td>
</tr>
<tr>
<td>Policy and Charging Application (PCA)</td>
<td>PCA Activation Procedure</td>
</tr>
<tr>
<td>Host Intrusion Detection System (HIDS)</td>
<td>DSR Security Guide, Section 3.2</td>
</tr>
<tr>
<td>Diameter Custom Applications (DCA)</td>
<td>DCA Framework and Application Activation and Deactivation Guide</td>
</tr>
</tbody>
</table>

### 4. Software Installation Procedure

As mentioned earlier, the host configuration and virtual networks should be done before executing the procedures in this document. It is assumed that at this point the user has access to:

- Consoles of all guests and hosts at all sites
- ssh access to the guests at all sites
- GUI access to hosts at all sites
- A configuration station with a web browser, ssh client, and scp client
- VM Manager Privileges to add OVA’s to catalog (VMware only)
- KVM/OpenStack admin and tenant privileges
- OVM-S/OVM-M credentials and privileges, OVM-M cli tool must be installed and is accessible

**SUDO**

As a non-root user (admusr), many commands (when run as admusr) now require the use of **sudo**.

**VIP/TSA (OpenStack Only)**

OpenStack release Kilo or later is required to configure VIP and target set addresses. Kilo release 2015.1.2 or later is preferred.

**IPv6**

IPv6 configuration of XMI and IMI networks has been introduced in DSR 7.1. Standard IPv6 formats for IPv6 and prefix can be used in all IP configuration screens, which enable the DSR to be run in an IPv6 only environment. When using IPv6 for XMI and management, you must place the IPv6 address in brackets (highlighted in red below), example as followed:

`https://[<IPv6 address>]`

If a dual-stack (IPv4 and IPv6) network is required, configure the topology with IPv4 first, and then “migrate” to IPv6. Reference [21] DSR IPv6 Migration Guide for instructions on how to accomplish this migration.
4.1 Create DSR Guests (VMware)

Procedure 1. (VMware) Import DSR OVA

This procedure adds the DSR OVA to the VMware catalog or repository. Check off (✓) each step as it is completed. Steps with shaded boxes require user input. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. Add DSR OVA image
   1. Launch the VMware client of your choice.
   2. Add the DSR OVA image to the VMware catalog or repository. Follow the instructions provided by the Cloud solutions manufacturer.

Procedure 2. (VMware only) Configure NOAM Guests Role Based On Resource Profile and Configure Network

This procedure configures networking on VMs. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, My Oracle Support (MOS) and ask for assistance.

1. Create the NOAM1 VM from the OVA image
   1. Browse the library or repository that you placed the OVA image.
   2. Deploy the OVA Image using vSphere Client or vSphere Web Client.
   3. Name the NOAM1 VM and select the data store.

2. Configure resources for the NOAM1 VM
   Configure the NOAM1 per the resource profiles defined in [27] DSR Cloud Benchmarking Guide for the DSR NOAM using the vSphere Client or vSphere Web Client.

3. Power on NOAM1
   Use the vSphere Client or vSphere Web Client to power on the NOAM1 VM.

4. Configure NOAM1
   1. Access the NOAM1 VM console via the vSphere Client or vSphere Web Client.
   2. Login as the admusr user.
   3. Set the <ethX> device:
      
      **Note:** Where ethX is the interface associated with the XMI network.
      
      $ sudo netadm add --device=<ethX> --address=<IP Address in External management Network> --netmask=<Netmask> --onboot=yes --bootproto=none
   4. Add the default route for ethX:
      
      $ sudo netadm add --route=default --gateway=<gateway address for the External management network> --device=<ethX>
   5. Ping the XMI gateway for network verification.
      
      $ ping -c3 <Gateway of External Management Network>
### Procedure 2. (VMware only) Configure NOAM Guests Role Based On Resource Profile and Configure Network

<table>
<thead>
<tr>
<th>Step #</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Configure NOAM2</td>
<td>Repeat steps 1 through 4 for the NOam2 VM.</td>
</tr>
</tbody>
</table>

### Procedure 3. (VMware only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network

<table>
<thead>
<tr>
<th>Step #</th>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create the SOAM1 VM from the OVA image</td>
<td>This procedure adds network addresses for all VMs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Note:</em> This procedure provides an example for creating an SOAM. Follow the same steps to create other guests with their respective VM names and profiles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td>1.</td>
<td>Browse the library or repository that you placed the OVA image.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Deploy the OVA image using vSphere Client or vSphere Web Client.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Name the SOAM1 VM and select the data store.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Configure resources for the SOAM1 VM</td>
<td>Configure the SOAM1 VM per the resource profiles defined in [27] DSR Cloud Benchmarking Guide for the DSR SO using the vSphere Client or vSphere Web Client. Interfaces must be added per the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.</td>
</tr>
<tr>
<td>3.</td>
<td>Power on SOAM1 VM</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Power on the DSR SOAM1 VM with the vSphere Client or vSphere Web Client.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Monitor the vApps screen's Virtual Machines tab until the DSR VM reports Powered On in the Status column.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td>Configure XMI interface</td>
<td>Access the VM console via the vSphere Client or vSphere Web Client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Login as the admusr user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set the ethX device:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Note:</em> Where ethX is the interface associated with the XMI network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo netAdm add --device=&lt;ethX&gt; --address=&lt;IP Address in External Management Network&gt; --netmask=&lt;Netmask&gt; --onboot=yes --bootproto=none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Add the default route for ethX:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo netAdm add --route=default --gateway=&lt;gateway address for the External management network&gt; --device=&lt;ethX&gt;</td>
</tr>
<tr>
<td>5.</td>
<td>Verify network connectivity</td>
<td>Access the SOAM1 VM console using the vSphere Client or vSphere Web Client.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Login as the admusr user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ping the NOAM1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ ping -c3 &lt;IP Address in External Management Network&gt;</td>
</tr>
</tbody>
</table>
Procedure 3. (VMware only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network

6. Procedure overview

Repeat steps 1 through 5 for the following VMs. Use unique labels for the VM names:
- MP(s)
- MP(s) SS7 (Optional Components)
- IPFE(s)
- SOAM(s)
- Session SBRs, Binding SBR (Optional Components)
- DR NOAMs (Optional Components)

4.2 Create DSR Guests (KVM/OpenStack)

Procedure 4. Import DSR OVA (KVM/OpenStack Only)

1. Preparation

1. Create instance flavors.

If not yet done, use the resource profiles defined in [27] DSR Cloud Benchmarking Guide values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the Admin section, or with the nova flavor-create command line tool. Make the flavor names as informative as possible. As flavors describe resource sizing, a common convention is to use a name like "0406060" where the first two figures (04) represent the number of virtual CPUs, the next two figures (06) might represent the RAM allocation in GB and the final three figures (060) might represent the disk space in GB.

2. If using an Intel 10 Gigabit Ethernet ixgbe driver on the host nodes, please note that the default LRO (Large Receive Offload) option must be disabled on the host command line. Please see the Intel release notes for more details. This action can be performed with the following command.

   $ sudo ethtool -K <ETH_DEV> lro off

3. If using IPFE Target Set Addresses (TSA):
   a. Read and understand Disable Port Security in Appendix F.6, including the warning note.
   b. Enable the Neutron port security extension.
Procedure 4. Import DSR OVA (KVM/OpenStack Only)

2. [ ] Add DSR OVA image

   1. Copy the OVA file to the OpenStack control node.
      
      $ scp DSR-x.x.x.x.ova admusr@node:~

   2. Log into the OpenStack control node.
      
      $ ssh admusr@node

   3. In an empty directory, unpack the OVA file using `tar`.
      
      $ tar xvf DSR-x.x.x.x.ova

   4. One of the unpacked files has a `.vmdk` suffix. This is the VM image file that must be imported.
      
      DSR-x.x.x.x-disk1.vmdk

   5. Source the OpenStack `admin` user credentials.
      
      $ . keystonerc_admin

   6. Select an informative name for the new image.
      
      dsr-8.1.x.x.x-original

   7. Import the image using the `glance` utility from the command line.
      
      $ glance image-create --name dsr-x.x.x.x-original --visibility public --protected false --progress --container-format bare --disk-format vmdk --file DSR-x.x.x.x-disk1.vmdk

   This process takes about 5 minutes depending on the underlying infrastructure.

Procedure 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile

<table>
<thead>
<tr>
<th>STEP #</th>
<th>This procedure configures networking on VMs. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. [ ] Name the new VM instance</td>
<td>1. Create an informative name for the new instance: <strong>NOAM1</strong>. 2. Examine the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.</td>
</tr>
</tbody>
</table>
### Procedure 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile

<table>
<thead>
<tr>
<th>OpenStack Control Node:</th>
<th>1. Get the following configuration values.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create and boot the NOAM VM instance from the glance image</td>
<td>a. The image ID.</td>
</tr>
<tr>
<td></td>
<td>* $ glance image-list*</td>
</tr>
<tr>
<td></td>
<td>b. The flavor ID.</td>
</tr>
<tr>
<td></td>
<td>* $ nova flavor-list*</td>
</tr>
<tr>
<td></td>
<td>c. The network ID(s)</td>
</tr>
<tr>
<td></td>
<td>* $ neutron net-list*</td>
</tr>
<tr>
<td></td>
<td>d. An informative name for the instance.</td>
</tr>
<tr>
<td></td>
<td>* NOAM1*</td>
</tr>
<tr>
<td></td>
<td>* NOAM2*</td>
</tr>
</tbody>
</table>

2. Create and boot the VM instance.

The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. Use one `--nic` argument for each IP/interface. Number of IP/interfaces for each VM type must conform with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.

**Note:** IPv6 addresses should use the `v6-fixed-ip` argument instead of `v4-fixed-ip`.

```
$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> <instance name>
```

3. View the newly created instance using the nova tool.

```
$ nova list --all --tenants
```

The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.

<table>
<thead>
<tr>
<th>OpenStack Control Node:</th>
<th>Note: Refer to Application VIP Failover Options (OpenStack) in Appendix F for more information on VIP.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure NOAM VIP (Optional)</td>
<td>If an NOAM VIP is needed, execute the following commands:</td>
</tr>
<tr>
<td></td>
<td>1. Find the port ID associated with the NOAM instance XMI interface.</td>
</tr>
<tr>
<td></td>
<td>* $ neutron port-list*</td>
</tr>
<tr>
<td></td>
<td>2. Add the VIP IP address to the address pairs list of the NOAM instance XMI interface port.</td>
</tr>
<tr>
<td></td>
<td>* $ neutron port-update &lt;Port ID&gt; --allowed_address_pairs list=true type=dict ip_address=&lt;VIP address to be added&gt;*</td>
</tr>
</tbody>
</table>

4. Check if interface is configured

If DHCP is enabled on the Neutron subnet, VM configures the VNIC with the IP address provided in step 2. To verify, ping the XMI IP address provided with the `nova boot` command from step 2:

```
$ ping <XMI-IP-Provided-During-Nova-Boot>
```

If the ping is successful, ignore step 5. to configure the interface manually.
Procedure 5. (KVM/OpenStack Only) Configure NOAM Guests Role Based on Resource Profile

5. OpenStack Dashboard (Horizon):
   Manually configure interface, if not already done (Optional)

   **Note:** If the instance is already configured with an interface and has successfully pinging (step 4.), then **ignore** this step to configure the interface manually.

   1. Log into the **Horizon** GUI as the DSR tenant user.
   2. Go to the Compute/Instances section.
   3. Click the **Name** field of the newly created instance.
   4. Select the Console tab.
   5. Login as the **admusr** user.

   6. Configure the network interfaces, conforming with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
      
      ```
      $ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask>
      $ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>
      ```

      Verify network connectivity by pinging Gateway of XMI network.
      
      ```
      $ ping –c3 <XMI Gateway>
      ```

      Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.

   7. Reboot the NOAM VM. It takes approximately 5 minutes for the VM to complete rebooting.
      
      ```
      $ sudo init 6
      ```

      The new VM should now be accessible via both network and Horizon consoles.

6. Configure NOAM2

   Repeat steps 1 through 5 for NOAM2.

Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Name the new VM instance</td>
</tr>
<tr>
<td>2.</td>
<td>Create an informative name for the new instance: <strong>SOAM1</strong>.</td>
</tr>
<tr>
<td>3.</td>
<td>Examine the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.</td>
</tr>
</tbody>
</table>
Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network

1. Get the following configuration values.
   a. The image ID.
      $ glance image-list
   b. The flavor ID.
      $ nova flavor-list
   c. The network ID(s)
      $ neutron net-list
   d. An informative name for the instance.
      SOAM1
      SOAM2

2. Create and boot the VM instance.

   The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. Use one --nic argument for each IP/interface. Number of IP/interfaces for each VM type must conform with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.

   **Note:** IPv6 addresses should use the `v6-fixed-ip` argument instead of `v4-fixed-ip`.

   $ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> <instance name>

3. View the newly created instance using the nova tool.

   $ nova list --all-tenants

   The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.

   **Note:** Refer to Allowed Address Pairs in Appendix F.2 for more information on VIP.

   If an SOAM VIP is needed, execute the following commands:

   1. Find the port ID associated with the SOAM instance XMI interface.
      $ neutron port-list

   2. Add the VIP IP address to the address pairs list of the SOAM instance XMI interface port.
      $ neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>

   If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address provided in step 2 above.

   To verify, ping the XMI IP address provided with nova boot... command (step 2):
   $ ping <XMI-IP-Provided-During-Nova-Boot>

   If the ping is successful, ignore step 5 to configure the interface manually.

3. Configure SOAM VIP (Optional)

4. Check if interface is configured
Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td>Manually configure interface, if not already done (Optional)</td>
</tr>
<tr>
<td>6.</td>
<td>Verify network connectivity</td>
</tr>
<tr>
<td>7.</td>
<td>Procedure overview</td>
</tr>
</tbody>
</table>

**Note:** If the instance is already configured with an interface and successfully pinging (step 4), then **ignore** this step to configure the interface manually.

1. Log into the Horizon GUI as the DSR tenant user.
2. Go to the Compute/Instances section.
3. Click the **Name** field of the newly created instance.
4. Select the Console tab.
5. Login as the **admusr** user.
6. Configure the network interfaces, conforming with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.
   - $ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask>
   - $ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>

Verify network connectivity by pinging Gateway of XMI network.
   - $ ping -c3 <XMI Gateway>

Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.

7. Reboot the SOAM VM. It takes approximately 5 minutes for the VM to complete rebooting.
   - $ sudo init 6

The new VM should now be accessible via both network and Horizon consoles.

1. Access the **SOAM1 VM console** using the openstack.
2. Login as the **admusr** user.
3. Ping the NOAM1.
   - $ ping -c3 <IP Address in External Management Network>

Repeat steps 1 through 6 for the following VMs. Use unique labels for the VM names. Assign addresses to all desired network interfaces:
- MP(s)
- MP(s) SS7 (Optional Components)
- IPFE(s)
- MP vSTP (For vSTP configuration) (Optional Components)
- SOAM(s)
- Session SBRs, Binding SBR (Optional Components)
- DR NOAMs (Optional Components)
## 4.3 Create DSR Guests (OVM-S/OVM-M)

### Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

This procedure imports the DSR image. This procedure requires values for these variables:
- \(<\text{OVM-M IP}> = \text{IP address to access a sh prompt on the OVM server}\)
- \(<\text{URL to OVA}> = \text{link to a source for downloading the product image (.ova)}\)
- \(<\text{MyRepository name}> = \text{name of the repository in the OVM to hold the product image (.ova)}\)

Execution of this procedure discovers and uses the values of these variables:
- \(<\text{Virtual Appliance OVA ID}>\)
- \(<\text{OVA VM name_vm_vm}>\)
- \(<\text{OVM network id for (each subnet)}>\)
- \(<\text{OVM network name for (each subnet)}>\)

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Preparation: Access command line of OVM</td>
</tr>
</tbody>
</table>

Refer to Common OVM Manager Tasks (CLI) in Appendix D for setting up the platform.

1. Get the site-specific values for these variables (overwrite example).
   - \(<\text{OVM-M IP}> = 100.64.62.221\)

2. Use the respective value for \(<\text{OVM-M IP}>\) into the command.
   - \(\text{ssh -l admin <OVM-M IP> -p 10000}\)
     
   Example:
   
   \(\text{ssh -l admin 100.64.62.221 -p 10000}\)
   
Alternatively, use a terminal emulation tool like putty.
## Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

<table>
<thead>
<tr>
<th></th>
<th>OVM-M CLI: Import the VirtualAppliance/OVA</th>
</tr>
</thead>
</table>
| 1. | Get the site-specific values for these variables (overwrite example).<br>`<URL to OVA> = http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova`
`<MyRepository name> = XLab Utility Repo01`<br>2. Use the respective values for `<MyRepository name>` and `<URL to OVA>` into the command.<br>```<MyRepository name>='XLab Utility Repo01' url='http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova'```<br>Example:```OVM> importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova```<br>3. Execute the command and validate success.<br>4. Examine the screen results to find site-specific text for variables in these locations:<br>Command: `importVirtualAppliance Repository name='XLab Utility Repo01'`<br>```url=http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova```<br>Status: Success<br>Time: 2017-04-18 15:23:31,044 EDT<br>JobId: 1492543363365<br>Data:```id: 1128a1c6ce name: DSR-8.1.0.0.0_81.16.0.ova```<br>5. Use the respective values for values for these variables (overwrite example).<br>`<Virtual Appliance OVA ID> = 1128a1c6ce`
Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

3. **OVM-M CLI:** Get the virtual appliance ID

   - The virtual appliance OVA ID is used in later steps.
   - Get the site-specific text for these variables (overwrite example).
     
     \(<\text{Virtual Appliance OVA ID}> = 1128a1c6ce\)
   - Use the respective values for \(<\text{Virtual Appliance OVA ID}>\) into the command.
     
     \(\text{OVM}> \text{show VirtualAppliance id=}<\text{Virtual Appliance OVA id}>\)
   - Example:
     
     \(\text{OVM}> \text{show VirtualAppliance id=1128a1c6ce}\)
   - Execute the command and validate success.
   - Examine the screen results to find site-specific text for **variables** in these locations:
     
     Command: \(\text{show VirtualAppliance id=1128a1c6ce}\)
     
     Status: Success
     
     
     Data:
     
     Origin = http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova
     
     Repository = 0004fb0000030000da5738315337bfc7 [XLab Utility Repo01]
     
     Virtual Appliance Vm 1 = 11145510c0_vm_vm [vm]
     
     Virtual Appliance VirtualDisk 1 = 11145510c0_disk_disk1 [disk1]
     
     Id = 11145510c0 [DSR-8.1.0.0.0_81.16.0.ova]
     
     Name = DSR-8.1.0.0.0_81.16.0.ova
     
     Description = Import URL: http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova
     
     Locked = false
   - Use the respective values for these variables (overwrite example).
     
     \(<\text{OVA VM name_vm_vm}> = 11145510c0_vm_vm\)
Procedure 7. (OVM-S/OVM-M). Import DSR OVA and prepare for VM creation

4. OVM-M CLI:
   Determine the OVM network IDs (established during the platform installation)

   **OVM> list Network**

1. Execute the command and validate success.

2. Examine the screen results to find the find site-specific OVM values for each subnet:
   - `<OVM network ID>`
   - `<OVM network name>`

3. Note the entire screen results. Refer to this data in later steps.

   **Command: list network**
   **Status: Success**
   **Time: 2017-04-19 18:51:42,494 EDT**
   **Data:**

   ```
   id:10486545b5  name:XSI-7  (10.196.237.0/25)
   id:10f4d74d5c  name:XMI-11  (10.75.159.0/25)
   id:10775cf4e5  name:IDIH Internal
   id:102e89a481  name:IMI Shared  (169.254.9.0/24)
   id:c0a80500  name:192.168.5.0
   id:10d8de6d9a  name:XSI-6  (10.196.236.128/25)
   id:10806a91fb  name:XSI-8  (10.296.237.128/25)
   id:10a729aadd  name:Control DHCP
   id:1053a04f0  name:XSI-5  (10.196.236.0/25)
   id:10345112b9  name:XMI-10  (10.75.158.128/25)
   ```

4. Use the respective values for network ID variables (change the examples in table according to the values).

<table>
<thead>
<tr>
<th></th>
<th>OAM (XMI)</th>
<th>Local (IMI)</th>
<th>Signaling A (XSI1)</th>
<th>Signaling B (XSI2)</th>
<th>Signaling C (XSI3-16)</th>
<th>Replication (SBR Rep)</th>
<th>DIH Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;OVM network name&gt;</code></td>
<td>XMI-10</td>
<td>IMI Shared</td>
<td>XSI-5</td>
<td>XSI-6</td>
<td>XSI-7</td>
<td>DIH Internal</td>
<td>XMI-10</td>
</tr>
<tr>
<td><code>&lt;OVM network ID&gt;</code></td>
<td>10345112b9</td>
<td>102e89a481</td>
<td>1053a04f0</td>
<td>10d8de6d9a</td>
<td>10486554b5</td>
<td>10775c4e5</td>
<td></td>
</tr>
</tbody>
</table>
4.4 Configure Virtual Machines

Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>This procedure creates virtual machines. Repeat this procedure for each DSR VM guests that needs to be created. This procedure requires values for these variables:</td>
<td></td>
</tr>
<tr>
<td>• &lt;OVA VM name_vm_vm&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;ServerPool name&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;VM name&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;OVM network ID for XMI&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;OVM network ID for IMI&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;OVM network ID for XSI#&gt; where # is a numeric from 1-16, for the signaling networks</td>
<td></td>
</tr>
<tr>
<td>• &lt;OVM network ID for Replication XSI#&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;URL for OVM GUI&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;VM IP in XMI&gt; from the NAPD</td>
<td></td>
</tr>
<tr>
<td>• &lt;Gateway for XMI&gt; from the NAPD</td>
<td></td>
</tr>
<tr>
<td>• &lt;NetMask for XMI&gt; from the NAPD</td>
<td></td>
</tr>
<tr>
<td>Execution of this procedure discovers and uses the values of these variables:</td>
<td></td>
</tr>
<tr>
<td>• &lt;VM ID&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;vCPUs Production&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;VNIC 1 ID&gt;</td>
<td></td>
</tr>
<tr>
<td>• &lt;interface name&gt; defined in [27] DSR Cloud Benchmarking Guide</td>
<td></td>
</tr>
</tbody>
</table>

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. OVM-M CLI: Create a VM for each guest from the VM in the OVA virtual appliance
   1. Get the site-specific text for these variables (overwrite example).
      <OVA VM name_vm_vm> = 11145510c0_vm_vm
   2. Use the respective values for <OVA VM name> into the command.
      OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=<OVA VM name>
      Example:
      OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm
   3. Execute the command and validate success.
   4. Examine the screen results to find site-specific text for variables in these locations:
      Command: createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm
      Status: Success
**Procedure 8. (OVM-S/OVM-M). Configure each DSR VM**

<table>
<thead>
<tr>
<th>Time: 2017-04-18 16:02:09,141 EDT</th>
</tr>
</thead>
<tbody>
<tr>
<td>JobId: 1492545641976</td>
</tr>
</tbody>
</table>

**Data:**

- id: `0004fb0000060004a0e02bdf9fc1bcd` name: DSR-8.1.0.0.0.0_81.16.0.ova_vm

5. Use the respective values for these variables (overwrite example).

   - `<VM ID>` = `0004fb0000060004a0e02bdf9fc1bcd`

2. **OVM-M CLI: Add the VM to the server pool**

   1. Get the site-specific text for these variables (overwrite example).

      - `<VM ID>` = `0004fb0000060004a0e02bdf9fc1bcd`
      - `<ServerPool name>` = `XLab Pool 01`

   2. Use the respective values for `<VM ID>` and `<ServerPool name>` into the command.

      ```
      OVM> add Vm id=<VM id> to ServerPool name="<ServerPool name>"
      
      Example:
      OVM> add Vm id=0004fb0000060004a0e02bdf9fc1bcd to ServerPool name="XLab Pool 01"
      
      Command: add Vm id=0004fb0000060004a0e02bdf9fc1bcd to ServerPool name="XLab Pool 01"
      
      Status: Success
      
      Time: 2017-04-19 21:05:10,950 EDT
      
      JobId: 1492650310802
      ```

   3. Execute the command and validate success.

**Note:** Refer to the Server Pool section in Appendix D.2 for more information.
Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

1. Get the site-specific text for these variables (overwrite example).
   - `<VM ID> = 0004fb00000600004a0e02bdf9fcb1bcd`
   - `<VM name> = na-noam-na-2a`
   - `<vCPUs Production> = 4`


<table>
<thead>
<tr>
<th>VM Name</th>
<th>vCPUs Lab</th>
<th>RAM (GB) Lab</th>
<th>vCPUs Production</th>
<th>RAM (GB) Production</th>
<th>Storage (GB) Lab and Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of guest host</td>
<td>#</td>
<td>#</td>
<td>#</td>
<td>#</td>
<td>#</td>
</tr>
</tbody>
</table>

3. Use the respective values for `<VM ID>`, `<VM name>`, and `<vCPUs Production>` into the command.

   OVM> edit Vm id=<VM id> name=<VM name> memory=6144 memoryLimit=6144 cpuCountLimit=<vCPUs Production> cpuCount=<vCPUs Production> domainType=XEN_HVM description="<VM name>"

   Example:
   
   OVM> edit Vm id=0004fb00000600004a0e02bdf9fcb1bcd name=na-noam-na-2a memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4 domainType=XEN_HVM description="na-noam-na-2a"

4. Execute the command and validate success.

   Command: edit Vm id=0004fb00000600004a0e02bdf9fcb1bcd name=na-noam-na-2a memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4 domainType=XEN_HVM description="na-noam-na-2a"
   
   Status: Success
   
   Time: 2017-04-18 17:55:25,645 EDT
   
   JobId: 1492552525477

Now, the VM has a name and resources.

1. Get the site-specific text for these variables (overwrite example).
   - `<VM name> = na-noam-na-2a`

2. Use the respective value for `<VM name>` into the command.

   OVM> show Vm name=<VM name>

   Example:
   
   OVM> show Vm name=na-noam-na-2a

3. Execute the command and validate success.

4. Examine the screen results to find site-specific text for variables in these locations:
   
   Status = Stopped
   
   Memory (MB) = 6144
   
   Max. Memory (MB) = 6144
Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

- Processors = 4
- Max. Processors = 4
- Priority = 50
- Processor Cap = 100
- High Availability = No
- Operating System = Oracle Linux 6
- Mouse Type = PS2 Mouse
- Domain Type = Xen HVM
- Keymap = en-us
- Start Policy = Use Pool Policy
- Origin = http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova
- Disk Limit = 4
- Huge Pages Enabled = No
- Config File Absolute Path = 192.168.5.5:/storage/ovm01/repository/VirtualMachines/0004fb0000600004a0e02bdf9fc1bcd/vm.cfg
- Config File Mounted Path = /OVS/Repositories/0004fb000030000da5738315337bfc7/VirtualMachines/0004fb0000600004a0e02bdf9fc1bcd/vm.cfg
- Server Pool = 0004fb00000200009148c8926d307f05 [XLab Pool 01]
- Repository = 0004fb0000030000da5738315337bfc7 [XLab Utility Repo01]
- Vnic 1 = 0004fb000007000091e1ab5ae291d8a [Template Vnic]
- VmDiskMapping 1 = 0004fb0000130000a1996c6074d40563 [Mapping for disk Id (79def426328a4127b5bf9f7ae53d3f48.img)]
- VmDiskMapping 2 = 0004fb00001300002db3d467a143ab5 [Mapping for disk Id (EMPTY_CDROM)]
- Restart Action On Crash = Restart
- Id = 0004fb0000600004a0e02bdf9fc1bcd [na-noam-na-2a]
- Name = na-noam-na-2a
- Description = na-noam-na-2a
- Locked = false
- DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)]

5. Use the respective values for these variables (overwrite example).

<Vnic 1 ID> = 0004fb000007000091e1ab5ae291d8a


**Procedure 8. (OVM-S/OVM-M). Configure each DSR VM**

5. Determine network interfaces for the type of guest host

Refer to [27] DSR Cloud Benchmarking Guide to learn which network interfaces need to be configured for each guest type. The table looks like this:

<table>
<thead>
<tr>
<th>Type of guest host</th>
<th>OAM (XMI)</th>
<th>Local (IMI)</th>
<th>Sig A (XSI1)</th>
<th>Sig B (XSI2)</th>
<th>Sig C (XSI3-16)</th>
<th>Rep (SBR)</th>
<th>DIH Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
</tr>
</tbody>
</table>

**Note:** The VNICs need to be created in the correct order so the interfaces are associated with the correct network.

6. OVM-M CLI: Attach XMI VNIC (if required by guest host type)

Add (attach) VNIC ID of the XMI network to VM:

1. Get the site-specific text for these variables (overwrite example)
   
   `<VNIC 1 ID> = 0004fb000007000091e1ab5ae291d8a`
   
   `<OVM network ID for XMI> = 10345112c9`

2. Use the respective values for `<VNIC 1 ID>` and `<OVM network ID for XMI>` into the command

   `OVM> add Vnic ID=<Vnic 1 ID> to Network name=<OVM network ID for XMI>`

   Example:
   
   `OVM> add Vnic ID=0004fb000007000091e1ab5ae291d8a to Network name=10345112c9`

3. Execute the command and validate success.

   **Command:** `add Vnic id=0004fb000007000091e1ab5ae291d8a to Network name=10345112c9`
   
   **Status:** Success
   
   **Time:** 2017-04-19 19:08:59,496 EDT
   
   **JobId:** 1492643339327
### Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

<table>
<thead>
<tr>
<th></th>
<th>OVM-M CLI: Create and attach IMI VNIC (if required by guest host type)</th>
<th>Create VNIC ID on the IMI network and attach to VM:</th>
</tr>
</thead>
</table>
| 7. | **CLI:** Create and attach IMI VNIC (if required by guest host type) | 1. Get the site-specific text for these variables (overwrite example).  
   - `<VM name>` = `na-noam-na-2a`  
   - `<OVM network ID for IMI>` = `102e89a481`  
   2. Use the respective values for `<OVM network ID for IMI>` and `<VM name>` into the command.  
      - `OVM>` create Vnic network=<OVM network ID for IMI> name=<VM name>-IMI on Vm name=<VM name>  
        Example:  
        - `OVM>` create Vnic network=102e89a481 name=na-noam-na-2a-IMI on Vm name=na-noam-na-2a  
   3. Execute the command and validate success.  
      - `Command:` create Vnic network=102e89a481 name=na-noam-na-2a-IMI on Vm name=na-noam-na-2a  
      - `Status:` Success  
      - `JobId:` 1492651317194  
      - `Data:`  
        - `id:0004fb00000700004f16dc3bfe0750a7 name:na-noam-na-2a-IMI`  

<table>
<thead>
<tr>
<th></th>
<th>OVM-M CLI: Create and attach XSI VNIC(s) (if required by guest host type)</th>
<th>Create VNIC ID on the XSI network(s) and attach to VM:</th>
</tr>
</thead>
</table>
| 8. | **Note:** Repeat this step if the VM will have multiple signaling networks, specifying the number of the network | 1. Get the site-specific text for these variables (overwrite example).  
   - `<VM name>` = `hostname`  
   - `<OVM network ID for XSI#>` = `1053a604f0`  
   - `<#>` = `the number of the XSI network [1-16]`  
   2. Use the respective values for `<OVM network ID for XSI#>` and `<VM name>` into the command.  
      - `OVM>` create Vnic network=<OVM network id for XSI#> name=<VM name>-XSI<#> on Vm name=<VM name>  
        Example:  
        - `OVM>` create Vnic network=1053a604f0 name=hostname-XSI1 on Vm name=hostname  
   3. Execute the command and validate success.
### Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 9.   | **OVM-M CLI:** Create and attach replication VNIC (if required by guest host type)  
Create VNIC ID on the Replication network and attach to VM:  
1. Get the site-specific text for these variables (overwrite example).  
   - `<VM name>` = hostname  
   - `<OVM network ID for Replication XSI#>` = 10486554b5  
   - `<OVM network name for Replication XSI#>` = XSI7  
   - `<#>` = the number of the XSI Replication network [1-16]  
2. Use the respective values for `<OVM network ID for Replication XSI#>`, `<OVM network name for Replication XSI#>`, and `<VM name>` into the command.  
   - **Example:**  
   ```bash  
   OVM> create Vnic network=10486554b5 name=hostname-XSI7 on Vm name=hostname  
   ```  
3. Execute the command and validate success.  
   - **Example:**  
   ```bash  
   OVM> create Vnic network=10486554b5 name=hostname-XSI7 on Vm name=hostname  
   ```  
| 10.  | **OVM-M CLI:** Start VM  
Start VM:  
1. Get the site-specific text for these variables (overwrite example).  
   - `<VM name>` = na-noam-na-2a  
2. Use the respective values for `<VM name>` into the command.  
   - **Example:**  
   ```bash  
   OVM> start Vm name=na-noam-na-2a  
   ```  
3. Execute the command and validate success.  
   - **Example:**  
   ```bash  
   OVM> start Vm name=na-noam-na-2a  
   ```

Status: Success  
Time: 2017-04-19 19:29:35,376 EDT  
JobId: 1492644568558
### Procedure 8. (OVM-S/OVM-M). Configure each DSR VM

1. Get the site-specific text for these variables (overwrite example).
   - <URL for OVM GUI> = [https://100.64.62.221:7002/ovm/console/faces/resource/resourceView.jspx](https://100.64.62.221:7002/ovm/console/faces/resource/resourceView.jspx)
   - <interface name> = from the table in [27] DSR Cloud Benchmarking Guide
   - <VM IP in XMI> = from the NAPD
   - <Gateway for XMI> = from the NAPD
   - <NetMask for XMI> = from the NAPD

2. Access the CLI of the console for the VM:

3. Log into the OVM-M GUI by typing the `<URL for OVM GUI>` into a browser.
   - Navigate to the Servers and VMs tab.
   - Expand and select the `<ServerPool name>`.
   - From the Perspective list, select Virtual Machines.
   - Select the `<VM name>` from the rows listed, and click the Launch Console icon.
   - In the Console window, log into the VM as the admusr.

4. Use the respective values for `<interface name>`, `<VM IP in XMI>`, `<Gateway for XMI>`, and `<NetMask for XMI>` into the commands

   **XMI:**
   - `$ sudo netAdm set --onboot=yes --device=<interface name> --address=<VM IP in XMI> --netmask=<NetMask for XMI>`
   - `$ sudo netAdm add --route=default --device=<interface name> --gateway=<Gateway for XMI>`

   Example:
   - `$ sudo netAdm set --onboot=yes --device=eth0 --address=10.75.158.189 --netmask=255.255.255.128`
   - `$ sudo netAdm add --route=default --device=eth0 --gateway=10.75.158.129`

5. Execute the command and validate success

6. Verify network connectivity by pinging Gateway of network
   - `$ ping -c3 <Gateway for XMI>`

7. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.
   - `$ sudo init 6`

The new VM should now be accessible via both network and console.
4.5 Application Configuration

Procedure 9. Configure the First NOAM NE and Server

This procedure configures the first NOAM VM. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. NOAM GUI: Login
   Establish a GUI session as the guiaadmin user on the NOAM server by using the XMI IP address.

   ![Oracle System Login](image)

   - Username: [Input]
   - Password: [Input]
   - Change password
   
   Log In

   Welcome to the Oracle System Login.

   This application is designed to work with most modern HTML5 compliant browsers and uses both Javascript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

   Unauthorized access is prohibited.

   Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
Procedure 9. Configure the First NOAM NE and Server

1. Navigate to **Main Menu->Configuration->Networking->Networks.**

2. **NOAM GUI:** Create the NOAM network element using the XML file.

   - Click **Browse** and type the pathname of the NOAM network XML file.

   - Click **Upload File** to upload the XML file. See the examples in Appendix A Sample Network Element and Hardware Profiles and configure the NOAM network element.

   To create a new Network Element, upload a valid configuration file:

   ![Upload File]

   - Click **Upload File**

3. Once the data has been uploaded, you should see a tabs display with the name of your network element. Click on this tab which describes the individual networks that are now configured.
### Procedure 9. Configure the First NOAM NE and Server

#### 3. NOAM GUI: Map services to networks

1. Navigate to **Main Menu->Configuration->Networking->Services**.
2. Click **Edit** and set the services as shown in the table below:

<table>
<thead>
<tr>
<th>Name</th>
<th>Intra-NE Network</th>
<th>Inter-NE Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAM</td>
<td>&lt;IMI Network&gt;</td>
<td>&lt;XMI Network&gt;</td>
</tr>
<tr>
<td>Replication</td>
<td>&lt;IMI Network&gt;</td>
<td>&lt;XMI Network&gt;</td>
</tr>
<tr>
<td>Signaling</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
<tr>
<td>HA_Secondary</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
<tr>
<td>HA_MP_Secondary</td>
<td>Unspecified</td>
<td>Unspecified</td>
</tr>
<tr>
<td>Replication_MP</td>
<td>&lt;IMI Network&gt;</td>
<td>Unspecified</td>
</tr>
<tr>
<td>ComAgent</td>
<td>&lt;IMI Network&gt;</td>
<td>Unspecified</td>
</tr>
</tbody>
</table>

For example, if your IMI network is named **IMI** and your XMI network is named **XMI**, then your services configuration should look like the following:

![Services Configuration Diagram](image)

3. Click **OK** to apply the Service-to-Network selections. Dismiss any possible popup notifications.

#### 4. NOAM GUI: Insert the 1st NOAM VM

1. Navigate to **Main Menu->Configuration->Networking->Servers**.
2. Click **Insert** to insert the new NOAM server into servers table (the first or
Procedure 9. Configure the First NOAM NE and Server

server).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname *</td>
<td></td>
</tr>
<tr>
<td>Role *</td>
<td>- Select Role -</td>
</tr>
<tr>
<td>System ID</td>
<td></td>
</tr>
<tr>
<td>Hardware Profile</td>
<td>DSR Guest</td>
</tr>
<tr>
<td>Network Element Name *</td>
<td>- Unassigned -</td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
</tbody>
</table>

3. Fill in the fields as follows:

Hostname: <Hostname>
Role: NETWORK OAM&P
System ID: <Site System ID>
Hardware Profile: DSR Guest
Network Element Name: [Select NE from list]

The network interface fields are now available with selection choices based on the chosen hardware profile and network element.

OAM Interfaces [At least one interface is required]:

<table>
<thead>
<tr>
<th>Network</th>
<th>IP Address</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNAL/XMI (10.106.227.0/24)</td>
<td>10.106.227.21</td>
<td>v10</td>
</tr>
<tr>
<td>INTERNAL/XMI (169.254.1.0/24)</td>
<td>169.254.1.21</td>
<td>v11</td>
</tr>
</tbody>
</table>

4. Fill in the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.

5. Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.

6. Add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid NTP Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
</tbody>
</table>

7. Click OK when you have completed entering all the server data.
### Procedure 9. Configure the First NOAM NE and Server

#### 5. NOAM GUI: Export the initial configuration

1. Navigate to **Main Menu->Configuration->Networking->Servers.**

2. From the GUI screen, select the NOAM server and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.

#### 6. NOAM Server: Copy configuration file to 1st NOAM server

1. Obtain a terminal window to the 1st NOAM server, logging in as the **admusr** user.

2. Copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the 1st NOAM to the `/var/tmp` directory. The configuration file has a filename like `TKLCConfigData.<hostname>.sh`. The following is an example:

   ```
   $ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh
   ```

#### 7. First SOAM Server: Wait for configuration to complete

The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.

If you are on the console, wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure.

Verify the script completed successfully by checking the following file:

```
$ sudo cat /var/TKLC/appw/logs/Process/install.log
```

**Note:** Ignore the warning about removing the USB key since no USB key is present. No response occurs until the reboot prompt is issued.

#### 8. First SOAM Server: Set the time zone (Optional) and reboot the server

To change the system time zone, from the command line prompt, execute `set_ini_tz.pl`. The following command example uses the America/New_York time zone.

Replace, as appropriate, with the time zone you have selected for this installation. For a full list of valid time zones, see Appendix B List of Frequently Used Time Zones.

```
$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1
```

$ sudo init 6

Wait for server to reboot.
Procedure 9. Configure the First NOAM NE and Server

9. First NOAM Server: Verify server health
   1. Login into the NOAM1 as the admusr user.
   2. Execute the following command as admusr on the 1st NOAM server and make sure no errors are returned:

      $ sudo syscheck

      Running modules in class hardware...
      OK
      Running modules in class disk...
      OK
      Running modules in class net...
      OK
      Running modules in class system...
      OK
      Running modules in class proc...
      OK

      LOG LOCATION: /var/TKLC/log/syscheck/fail_log

Procedure 10. Configure the NOAM Server Group

   This procedure configures the NOAM server group. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. NOAM GUI: Login
   Establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type http://<NO1_XMI_IP_Address> as the URL. Login as the guiadmin user. If prompted by a security warning, click Continue to this Website to proceed.
Procedure 10. Configure the NOAM Server Group

1. Navigate to **Main Menu->Configuration->Networking->Server Groups**.

2. NOAM GUI: Enter NOAM server group data
   - **Navigate to** Main Menu->Configuration->Networking->Server Groups.

2. Click **Insert** and fill in the following fields:
   - **Server Group Name**: [Enter Server Group Name]
   - **Level**: A
   - **Parent**: None
   - **Function**: DSR (Active/Standby Pair)
   - **WAN Replication Connection Count**: Use Default Value

3. Click **OK** when all fields are filled in.
Procedure 10. Configure the NOAM Server Group

3. **NOAM GUI**: Edit the NOAM Server Group


   ![Main Menu](image)

2. Select the new server group and click **Edit**.

   ![Edit Button](image)

   Select the network element that represents the NOAM.

<table>
<thead>
<tr>
<th>Server</th>
<th>SG Inclusion</th>
<th>Preferred HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOAM</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3. In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Mark the **Include in SG** checkbox.

4. Leave other boxes unchecked.

5. Click **OK**.

4. **NOAM Server**: Verify NOAM VM role

1. From console window of the first NOAM VM, execute the `ha.mystate` command to verify the DbReplication and VIP items under the `resourceId` column has a value of Active under the role column.

   You may have to wait a few minutes for it to be in that state.

2. Press **Ctrl+C** to exit.

   Example:

   ```
   [admin@NO1 ~]$ ha.mystate
<table>
<thead>
<tr>
<th>resourceId</th>
<th>role</th>
<th>node</th>
<th>DC</th>
<th>subResources</th>
<th>lastUpdate</th>
</tr>
</thead>
<tbody>
<tr>
<td>DbReplication</td>
<td>Act/Act</td>
<td>A1348.092</td>
<td></td>
<td>0627:056750.672</td>
<td></td>
</tr>
<tr>
<td>VIP</td>
<td>Act/Act</td>
<td>A1348.092</td>
<td></td>
<td>0627:056750.672</td>
<td></td>
</tr>
<tr>
<td>ces/mcss/ces</td>
<td>Act/Act</td>
<td>A1348.092</td>
<td></td>
<td>0627:056750.672</td>
<td></td>
</tr>
<tr>
<td>CAPI_HELP_Proc</td>
<td>Act/008</td>
<td>A1348.092</td>
<td></td>
<td>0627:056750.625</td>
<td></td>
</tr>
<tr>
<td>LOROM_Proc</td>
<td>Act/008</td>
<td>A1348.092</td>
<td></td>
<td>0627:056755.715</td>
<td></td>
</tr>
<tr>
<td>CAPI_POPF_Proc</td>
<td>Act/Act</td>
<td>A1348.092</td>
<td></td>
<td>0627:056800.737</td>
<td></td>
</tr>
</tbody>
</table>
   ```
Procedure 10. Configure the NOAM Server Group

5. **NOAM GUI:**
   - Restart 1st NOAM VM

   1. From the NOAM GUI, navigate to **Main Menu->Status & Manage->Server.**

   2. Select the first NOAM server. **Click Restart.**

   3. **Click OK** on the confirmation screen and wait for restart to complete.

6. **NOAM Server:**
   - Set symmetric thresholds for VMs.
   - **Note:** These commands disable the message rate threshold alarms

   From console window of the first NOAM VM, execute the **iset** commands as **admusr.**

   `$ sudo iset -feventNumber='-1' SysMetricThreshold where metricId='RoutingMsgRate' and function='DIAM'`

   `$ sudo iset -feventNumber='-1' SysMetricThreshold where metricId='RxRbarMsgRate' and function='RBAR'`

   `$ sudo iset -feventNumber='-1' SysMetricThreshold where metricId='RxFabrMsgRate' and function='FABR'`

   `$ sudo iset -feventNumber='-1' SysMetricThreshold where metricId='RxCpaMsgRate' and function='CPA'`

   `$ sudo iset -feventNumber='-1' SysMetricThreshold where metricId='RxDmiwfMsgRate' and function='DM-IWF'`

   `$ sudo iset -feventNumber='-1' SysMetricThreshold where metricId='RxMdIwfIngressMsgRate' and function='MD-IWF'`
Procedure 11. Configure the Second NOAM Server

This procedure configures the second NOAM server.
Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. NOAM GUI: Login
   1. If not already done, establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type `http://<NO1_XMI_IP_Address>` as the URL.

2. Login as the `guiadmin` user.

2. NOAM GUI: Insert the 2nd NOAM VM
   1. Navigate to **Main Menu->Configuration->Networking->Servers**.

   ![Diagram of Main Menu structure]

   2. Click **Insert** to insert the new NOAM server into servers table (the first or server).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>- Select Role -</td>
</tr>
<tr>
<td>System ID</td>
<td></td>
</tr>
<tr>
<td>Hardware Profile</td>
<td>DSR Guest</td>
</tr>
<tr>
<td>Network Element Name</td>
<td>- Unassigned -</td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
</tbody>
</table>

3. Fill in the fields as follows:
   - Hostname: `<Hostname>`
   - Role: `NETWORK OAM&P`
   - System ID: `<Site System ID>`
   - Hardware Profile: `DSR Guest`
   - Network Element Name: `[Choose NE list]`

   The network interface fields are now available with selection choices based on the chosen hardware profile and network element.
Procedure 11. Configure the Second NOAM Server

4. Fill in the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.

5. Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.

6. Add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid NTP Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
</tbody>
</table>

7. Click OK when you have completed entering all the server data.

3. **NOAM GUI:** Export the initial configuration

   1. Navigate to **Main Menu->Configuration->Networking->Servers.**

      - From the GUI screen, select server just configured and click **Export** to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.

4. **First NOAM Server:** Copy configuration file to 2nd NOAM server

   1. Obtain a terminal session to the 1st NOAM as the admusr user.

   2. Login as the admusr user to the NO1 shell and issue the following commands:

      ```
      $ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh
      ```

      **Note:** ipaddr is the IP address of NOAM2 assigned to its ethx interface associated with the xmi network.
Procedure 11. Configure the Second NOAM Server

<table>
<thead>
<tr>
<th></th>
<th>Second NOAM Server: Wait for configuration to complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td><strong>Second NOAM Server</strong>: Wait for configuration to complete</td>
</tr>
<tr>
<td></td>
<td>1. Obtain a terminal session to the 2nd NOAM as the <em>admusr</em> user.</td>
</tr>
<tr>
<td></td>
<td>The automatic configuration daemon looks for the file named <code>TKLCCfgData.sh</code> in the <code>/var/tmp</code> directory, implements the configuration in the file, and prompts the user to reboot the server.</td>
</tr>
<tr>
<td></td>
<td>2. If you are on the console, wait to be prompted to reboot the server, but <strong>DO NOT</strong> reboot the server, it is rebooted later in this procedure.</td>
</tr>
<tr>
<td></td>
<td>3. Verify script completed successfully by checking the following file.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo cat /var/TKLC/appw/logs/Process/install.log</code></td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: Ignore the warning about removing the USB key since no USB key is present.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Second NOAM Server: Reboot the server</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>Second NOAM Server</strong>: Reboot the server</td>
</tr>
<tr>
<td></td>
<td>Obtain a terminal session to the 2nd NOAM as the <em>admusr</em> user.</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo init 6</code></td>
</tr>
<tr>
<td></td>
<td>Wait for server to reboot.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Second NOAM Server: Verify server health</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td><strong>Second NOAM Server</strong>: Verify server health</td>
</tr>
<tr>
<td></td>
<td>1. Log into the NOAM2 as <em>admusr</em> and wait.</td>
</tr>
<tr>
<td></td>
<td>2. Execute the following command as super-user on the 2nd NO server and make sure no errors are returned:</td>
</tr>
<tr>
<td></td>
<td><code>$ sudo syscheck</code></td>
</tr>
<tr>
<td></td>
<td><code>Running modules in class hardware... OK</code></td>
</tr>
<tr>
<td></td>
<td><code>Running modules in class disk... OK</code></td>
</tr>
<tr>
<td></td>
<td><code>Running modules in class net... OK</code></td>
</tr>
<tr>
<td></td>
<td><code>Running modules in class system... OK</code></td>
</tr>
<tr>
<td></td>
<td><code>Running modules in class proc... OK</code></td>
</tr>
<tr>
<td></td>
<td><strong>LOG LOCATION</strong>: <code>/var/TKLC/log/syscheck/fail_log</code></td>
</tr>
</tbody>
</table>
Procedure 12. Complete Configuring the NOAM Server Group

This procedure finishes configuring the NOAM Server Group.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>NOAM GUI: Edit the NOAM Server Group Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the GUI session on the first NOAM server, navigate to <strong>Main Menu-&gt;Configuration-&gt;Networking-&gt;Server Groups.</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Select the NOAM server group and click <strong>Edit.</strong></td>
</tr>
<tr>
<td>3.</td>
<td>Add the second NOAM server to the server group by marking the <strong>Include in SG</strong> checkbox for the second NOAM server. Click <strong>Apply.</strong></td>
</tr>
<tr>
<td>4.</td>
<td>Click <strong>Add</strong> to add a NOAM VIP. Type the VIP Address and click <strong>OK.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server</th>
<th>SG Inclusion</th>
<th>Preferred HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO1</td>
<td>Include in SG</td>
<td>Prefer server as spare</td>
</tr>
<tr>
<td>NO2</td>
<td>Include in SG</td>
<td>Prefer server as spare</td>
</tr>
</tbody>
</table>

1. From the GUI session on the first NOAM server, navigate to Main Menu->Configuration->Networking->Server Groups.
### Procedure 12. Complete Configuring the NOAM Server Group

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Establish GUI session on the NOAM VIP</td>
</tr>
<tr>
<td></td>
<td>Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the <code>guiadmin</code> user.</td>
</tr>
<tr>
<td>3.</td>
<td>Wait for remote database alarm to clear</td>
</tr>
<tr>
<td></td>
<td>Wait for the alarm ID 10200 &quot;Remote Database re-initialization in progress&quot; to be cleared before proceeding (Main Menu-&gt;Alarms &amp; Events-&gt;View Active).</td>
</tr>
</tbody>
</table>
## Procedure 12. Complete Configuring the NOAM Server Group

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>NOAM GUI:</strong> Restart 2nd NOAM VM</td>
</tr>
</tbody>
</table>

1. Navigate to **Main Menu->Status & Manage->Server** and select the second NOAM server.

   - Status & Manage
     - Network Elements
     - Server
     - HA
     - Database
     - KPIs
     - Processes

2. Click **Restart**.

3. Click **OK** on the confirmation screen.

   ![Confirmation Screen]

   Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the **Appl State as Enabled**.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.</td>
<td><strong>SDS can now be installed (Optional)</strong></td>
</tr>
</tbody>
</table>

If this deployment contains SDS, SDS can now be installed. Refer to document referenced in [6] SDS SW Installation and Configuration Guide, CGBU_010592.
## Procedure 13. Configure the DR NOAM NE and Server (Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Primary NOAM VIP GUI: Login</strong> Establish a GUI session on the primary NOAM server by using the XMI VIP IP address.</td>
</tr>
</tbody>
</table>

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
Procedure 13. Configure the DR NOAM NE and Server (Optional)

2. **Primary NOAM VIP GUI**: Create the DR NOAM network element using the XML file

   1. Navigate to **Main Menu->Configuration->Networking->Networks**.

   2. **Primary NOAM VIP GUI**: Create the DR NOAM network element using the XML file

   3. **Primary NOAM VIP GUI**: Insert the 1st DR NOAM VM

   4. **Primary NOAM VIP GUI**: Insert the 1st DR NOAM VM

3. **Primary NOAM VIP GUI**: Insert the 1st DR NOAM VM

   1. Navigate to **Main Menu->Configuration->Networking->Servers**.

   2. Click **Insert** to insert the new NOAM server into servers table (the first or server).
Procedure 13. Configure the DR NOAM NE and Server (Optional)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>&lt;Hostname&gt;</td>
</tr>
<tr>
<td>Role</td>
<td>- Select Role -</td>
</tr>
<tr>
<td>System ID</td>
<td></td>
</tr>
<tr>
<td>Hardware Profile</td>
<td>DSR Guest</td>
</tr>
<tr>
<td>Network Element Name</td>
<td>- Unassigned -</td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
</tbody>
</table>

3. Fill in the fields as follows:
   - Hostname: <Hostname>
   - Role: NETWORK OAM&P
   - System ID: <Site System ID>
   - Hardware Profile: DSR Guest
   - Network Element Name: [Select NE from list]

The network interface fields are now available with selection choices based on the chosen hardware profile and network element.

4. Fill in the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.

5. Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unchecked.

6. Add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid NTP Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
</tbody>
</table>

7. Click OK when you have completed entering all the server data.
## Procedure 13. Configure the DR NOAM NE and Server (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Task Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Export the initial configuration</td>
</tr>
<tr>
<td></td>
<td>2. From the GUI screen, select the NOAM server and click Export to generate the initial configuration data for that server. Go to the Info tab to confirm the file has been created.</td>
</tr>
<tr>
<td>5.</td>
<td><strong>Primary NOAM Server:</strong> Copy configuration file to 1st NOAM server</td>
</tr>
<tr>
<td></td>
<td>1. Obtain a terminal window to the Primary NOAM server, logging in as the admusr user.</td>
</tr>
<tr>
<td></td>
<td>2. Copy the configuration file created in the previous step from the /var/TKLC/db/filemgmt directory on the 1st NOAM to the /var/tmp directory. The configuration file has a filename like TKLCConfigData.&lt;hostname&gt;.sh. The following is an example:</td>
</tr>
<tr>
<td></td>
<td>$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.&lt;hostname&gt;.sh /var/tmp/TKLCConfigData.sh</td>
</tr>
<tr>
<td>6.</td>
<td><strong>First DR NOAM Server:</strong> Wait for configuration to complete</td>
</tr>
<tr>
<td></td>
<td>The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and prompts the user to reboot the server.</td>
</tr>
<tr>
<td></td>
<td>If you are on the console, wait to be prompted to reboot the server, but <strong>DO NOT</strong> reboot the server, it is rebooted later in this procedure.</td>
</tr>
<tr>
<td></td>
<td>Verify the script completed successfully by checking the following file.</td>
</tr>
<tr>
<td></td>
<td>$ sudo cat /var/TKLC/appw/logs/Process/install.log</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Ignore the warning about removing the USB key since no USB key is present. No response occurs until the reboot prompt is issued.</td>
</tr>
<tr>
<td>7.</td>
<td><strong>First DR NOAM Server:</strong> Reboot the server</td>
</tr>
<tr>
<td></td>
<td>Obtain a terminal window to the 1st DR NOAM server, logging in as the admusr user.</td>
</tr>
<tr>
<td></td>
<td>$ sudo init 6</td>
</tr>
<tr>
<td></td>
<td>Wait for server to reboot.</td>
</tr>
</tbody>
</table>
### Procedure 13. Configure the DR NOAM NE and Server (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>First DR NOAM Server</th>
<th>Verification Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td></td>
<td>1. Obtain a terminal window to the 1&lt;sup&gt;st&lt;/sup&gt; DR NOAM server, logging in as the <strong>admusr</strong> user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Execute the following command as admusr and make sure that no errors are returned:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ sudo syscheck</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Running modules in class hardware... OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Running modules in class disk... OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Running modules in class net... OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Running modules in class system... OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Running modules in class proc... OK</td>
</tr>
<tr>
<td></td>
<td></td>
<td>LOG LOCATION: /var/TKLC/log/syscheck/fail_log</td>
</tr>
</tbody>
</table>

### Procedure 14. Configure the DR NOAM Server Group (Optional)

<table>
<thead>
<tr>
<th>Step #</th>
<th>Primary NOAM VIP GUI</th>
<th>Verification Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
<td>1. Establish a GUI session on the primary NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type <strong>http://&lt;NO1_XMI_IP_Address&gt;</strong> as the URL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Login as the <strong>gadmin</strong> user. If prompted by a security warming, click <strong>Continue to this Website</strong> to proceed.</td>
</tr>
</tbody>
</table>
Procedure 14. Configure the DR NOAM Server Group (Optional)

1. Using the GUI session on the primary NOAM server, navigate to **Main Menu->Configuration->Networking->Server Groups**.

2. Click **Insert** and fill in the following fields:
   - **Server Group Name**: [Enter Server Group Name]
   - **Level**: A
   - **Parent**: None
   - **Function**: DSR (Active/Standby Pair)
   - **WAN Replication Connection Count**: Use Default Value

3. Click **OK** when all fields are filled in.
Procedure 14. Configure the DR NOAM Server Group (Optional)

3. **Primary NOAM VIP GUI**: Edit the DR NOAM server group


2. Select the new server group and click **Edit**.

3. Select the network element that represents the DR NOAM.

<table>
<thead>
<tr>
<th>Server</th>
<th>SG Inclusion</th>
<th>Preferred HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSRDNOAM1</td>
<td>Include in SG</td>
<td></td>
</tr>
</tbody>
</table>

4. In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Mark the **Include in SG** checkbox.

5. Leave other boxes unchecked.

6. Click **OK**.

4. **Primary NOAM VIP GUI**: Restart 1\textsuperscript{st} DR NOAM VM

1. From the NOAM GUI, navigate to Main Menu->Status & Manage->Server.

2. Select the first NOAM server. Click **Restart**.

3. Click **OK** on the confirmation screen and wait for restart to complete.
Procedure 14. Configure the DR NOAM Server Group (Optional)

5. **NOAM Server:** Set symmetric threshold for VMs.
   
   *Note:* These commands disable the message rate threshold alarms.
   
   From console window of the first NOAM VM, execute the `iset` commands as `admusr`.
   
   ```bash
   sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RoutingMsgRate' and function='DIAM'"
   
   sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxRbarMsgRate' and function='RBAR'"
   
   sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxFabrMsgRate' and function='FABR'"
   
   sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxFabrMsgRate' and function='FABR'"
   
   sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxCpaMsgRate' and function='CPA'"
   
   sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxDmiwfMsgRate' and function='D-M-IWF'"
   
   sudo iset -feventNumber='-1' SysMetricThreshold where "metricId='RxMdIwfIngressMsgRate' and function='MD-IWF'"
   ```

Procedure 15. Configure the Second DR NOAM Server (Optional)

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>This procedure configures the second DR NOAM server. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td>1.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Login</td>
</tr>
<tr>
<td></td>
<td>If not already done, establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type <code>http://&lt;NOAM1_XMI_IP_Address&gt;</code> as the URL.</td>
</tr>
<tr>
<td></td>
<td>2. Login as the <code>guiadmin</code> user.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Insert the 2nd DR NOAM VM</td>
</tr>
<tr>
<td></td>
<td>1. Navigate to <strong>Main Menu -&gt; Configuration -&gt; Networking-&gt;Servers.</strong></td>
</tr>
<tr>
<td></td>
<td>2. Click <strong>Insert</strong> to insert the new NOAM server into servers table (the first or second server).</td>
</tr>
</tbody>
</table>
Procedure 15. Configure the Second DR NOAM Server (Optional)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td></td>
</tr>
<tr>
<td>Role</td>
<td>- Select Role -</td>
</tr>
<tr>
<td>System ID</td>
<td></td>
</tr>
<tr>
<td>Hardware Profile</td>
<td>DSR Guest</td>
</tr>
<tr>
<td>Network Element Name</td>
<td>- Unassigned -</td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
</tbody>
</table>

3. Fill in the fields as follows:
   - Hostname: <Hostname>
   - Role: NETWORK OAM&P
   - System ID: <Site System ID>
   - Hardware Profile: DSR Guest
   - Network Element Name: [Choose NE from list]

The network interface fields are now available with selection choices based on the chosen hardware profile and network element.

4. Fill in the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.

5. Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.

6. Add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid NTP Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
</tbody>
</table>

7. Click OK when you have completed entering all the server data.
Procedure 15. Configure the Second DR NOAM Server (Optional)

3. **Primary NOAM VIP GUI:** Export the initial configuration


      ![Main Menu]

      - Administration
      - Configuration
      - Networking
      - Servers
      - Server Groups
      - Resource Domains
      - Places
      - Place Associations

   2. From the GUI screen, select the server just configured and click Export to generate the initial configuration data for that server.

   3. Go to the Info tab to confirm the file has been created.

4. **Primary NOAM:** Copy configuration file to 2nd DR NOAM server

   1. Obtain a terminal session to the primary NOAM as the admusr user.

   2. Login as the admusr user to the NOAM1 shell and issue the following commands:

      ```
      $ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh
      ```

      **Note:** ipaddr is the IP address of DR NOAM assigned to its ethx interface associated with the XMI network.

5. **Second DR NOAM Server:** Wait for configuration to complete

   1. Obtain a terminal session to the 2nd DR NOAM as the admusr user.

      The automatic configuration daemon looks for the file named TKLCConfigData.sh in the /var/tmp directory, implements the configuration in the file, and prompts the user to reboot the server.

   2. If you are on the console, wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure.

   3. Verify script completed successfully by checking the following file.

      ```
      $ sudo cat /var/TKLC/appw/logs/Process/install.log
      ```

      **Note:** Ignore the warning about removing the USB key since no USB key is present.

6. **Second DR NOAM Server:** Reboot the server

   1. Obtain a terminal session to the 2nd DR NOAM as the admusr user.

      ```
      $ sudo init 6
      $ sudo init 6
      ```

      Wait for server to reboot.
Procedure 15. Configure the Second DR NOAM Server (Optional)

1. Obtain a terminal session to the 2nd DR NOAM as the `admusr` user.
2. Execute the following command as super-user and make sure no errors are returned:
   
   ```
   $ sudo syscheck
   Running modules in class hardware...  OK
   Running modules in class disk...      OK
   Running modules in class net...       OK
   Running modules in class system...    OK
   Running modules in class proc...      OK
   LOG LOCATION: /var/TKLC/log/syscheck/fail_log
   ```
## Procedure 16. Complete Configuring the DR NOAM Server Group (Optional)

This procedure finishes configuring the DR NOAM Server Group.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>PRIMARY NOAM VIP GUI: Edit the DR NOAM server group data</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>From the GUI session on the primary NOAM server, navigate to <strong>Main Menu-&gt;Configuration-&gt;Networking-&gt;Server Groups.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="diagram.png" alt="Diagram" /></td>
</tr>
<tr>
<td></td>
<td>2. Select the NOAM server group and click <strong>Edit.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="edit_button.png" alt="Edit Button" /></td>
</tr>
<tr>
<td></td>
<td>3. Add the second NOAM server to the server group by marking the <strong>Include in SG</strong> checkbox for the second NOAM server. Click <strong>Apply.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="Checkbox.png" alt="Checkbox" /></td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add</strong> to add an NOAM VIP. Type the <strong>VIP Address</strong> and click <strong>OK.</strong></td>
</tr>
<tr>
<td></td>
<td><img src="VIP_Assignment.png" alt="VIP Assignment" /></td>
</tr>
</tbody>
</table>
### Procedure 16. Complete Configuring the DR NOAM Server Group (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Establish GUI Session on the NOAM VIP</td>
</tr>
<tr>
<td></td>
<td>Establish a GUI session on the primary NOAM by using the NOAM VIP address. Login as the <strong>guiadmin</strong> user.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Oracle System Login" /></td>
</tr>
<tr>
<td>3.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Wait for Remote Database Alarm to Clear</td>
</tr>
<tr>
<td></td>
<td>Wait for the alarm ID 10200 &quot;Remote Database re-initialization in progress&quot; to be cleared before proceeding (<strong>Main Menu-&gt;Alarms &amp; Events-&gt;View Active</strong>)</td>
</tr>
</tbody>
</table>
Procedure 16. Complete Configuring the DR NOAM Server Group (Optional)

4. Primary NOAM VIP GUI: Restart 2nd DR NOAM VM

1. Navigate to Main Menu->Status & Manage->Server and select the second DR NOAM server.

2. Click Restart.

3. Answer OK on the confirmation screen.

Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the Appl State as Enabled.

5. Primary NOAM: Modify DSR OAM process

Establish an SSH session to the primary NOAM, login as the admusr user. Execute the following commands:

1. Retrieve the cluster ID of the DR-NOAM:

   `$ sudo iqt --NodeID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>'"`

<table>
<thead>
<tr>
<th>Server_ID</th>
<th>NodeID</th>
<th>ClusterID</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Oahu-DSR-DR-NOAM-2</td>
<td>A1055</td>
</tr>
</tbody>
</table>

2. Execute the following command to start the DSR OAM process on the DR-NOAM.

   `$ echo "|DSROAM Proc|Yes" | iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg`
## Procedure 17. Configure the SOAM NE

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Establish GUI session on the NOAM VIP. If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the guiadmin user.</td>
</tr>
</tbody>
</table>

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
Procedure 17. Configure the SOAM NE

2. **Primary NOAM VIP GUI**: Create the SOAM network element using an XML file

Make sure to have an SOAM network element XML file available on the PC running the web browser. The SOAM network element XML file is similar to what was created and used in Procedure 9, but defines the SOAM network element.

Refer to Appendix A Sample Network Element and Hardware Profiles for a sample network element xml file

1. Navigate to **Main Menu->Configuration->Networking->Networks**.

   ![Main Menu](image)

   1. Click **Browse** and type the path and name of the SOAM network XML file.

   ![Browse](image)

   2. Click **Upload** to upload the XML file and configure the SOAM network element.
### Procedure 18. Configure the SOAM Servers

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Establish GUI session on the NOAM VIP. If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the <code>guiadmin</code> user.</td>
</tr>
<tr>
<td>2.</td>
<td><strong>Primary NOAM VIP GUI:</strong> Insert the 1st SOAM server</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Main Menu-&gt;Status &amp; Manage-&gt;Server.</strong></td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Insert</strong> to insert the new SOAM server into servers table.</td>
</tr>
</tbody>
</table>
Procedure 18. Configure the SOAM Servers

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>&lt;SO1-Hostname&gt;</td>
</tr>
<tr>
<td>Role</td>
<td>SYSTEM OAM</td>
</tr>
<tr>
<td>System ID</td>
<td>&lt;Site System ID&gt;</td>
</tr>
<tr>
<td>Hardware Profile</td>
<td>DSR Guest</td>
</tr>
<tr>
<td>Network Element Name</td>
<td>[Choose NE from list]</td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
</tbody>
</table>

3. Fill in the fields as follows:
   - Hostname: <SO1-Hostname>
   - Role: SYSTEM OAM
   - System ID: <Site System ID>
   - Hardware Profile: DSR Guest
   - Network Element Name: [Choose NE from list]

The network interface fields are now available with selection choices based on the chosen hardware profile and network element.

<table>
<thead>
<tr>
<th>OAM Interfaces (At least one interface is required)</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network:</td>
<td>IP Address</td>
</tr>
<tr>
<td>INTERNALXM (16.196.227.0/24)</td>
<td>10.196.227.23</td>
</tr>
<tr>
<td>INTERNALMI (169.254.1.0/24)</td>
<td>169.254.1.23</td>
</tr>
</tbody>
</table>

4. Fill in the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.

5. Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.

6. Add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid NTP Server</td>
<td>Yes</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
<tr>
<td>Valid NTP Server</td>
<td>No</td>
</tr>
</tbody>
</table>

7. Click OK when you have completed entering the server data.
Procedure 18. Configure the SOAM Servers

3. **Primary NOAM VIP GUI:** Export the initial configuration

   1. Navigate to **Main Menu > Status & Manage > Server.**
   2. From the GUI screen, select the desired server and click **Export** to generate the initial configuration data for that server.
   3. Go to the Info tab to confirm the file has been created.

4. **Primary NOAM:** Copy configuration file to the 1st SOAM server

   Login as the **admusr** user to the NOAM1 shell and issue the commands:
   ```bash
   $ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh
   ```

   1. Obtain a terminal session on the 1st SOAM as the **admusr** user.
   2. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the /var/tmp directory, implements the configuration in the file, and prompts the user to reboot the server.
   3. If you are on the console wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure.
   4. Verify script completed successfully by checking the following file.
      ```bash
      $ sudo cat /var/TKLC/appw/logs/Process/install.log
      ```
      **Note:** Ignore the warning about removing the USB key since no USB key is present.

5. **First SOAM Server:** Wait for configuration to complete

6. **First SOAM Server:** Reboot the server

   Obtain a terminal session to the 1st SOAM as the **admusr** user.
   ```bash
   $ sudo init 6
   ```
   Wait for server to reboot.
### Procedure 18. Configure the SOAM Servers

<table>
<thead>
<tr>
<th></th>
<th>First SOAM Server: Verify Server Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td><strong>First SOAM Server: Verify Server Health</strong></td>
</tr>
<tr>
<td></td>
<td>1. After the system reboots, login again as the <strong>admusr</strong> user.</td>
</tr>
<tr>
<td></td>
<td>2. Execute the following command and make sure that no errors are returned:</td>
</tr>
<tr>
<td></td>
<td># sudo syscheck</td>
</tr>
<tr>
<td></td>
<td>Running modules in class hardware...</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Running modules in class disk...</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Running modules in class net...</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Running modules in class system...</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>Running modules in class proc...</td>
</tr>
<tr>
<td></td>
<td>OK</td>
</tr>
<tr>
<td></td>
<td>LOG LOCATION: /var/TKLC/log/syscheck/fail_log</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Insert and Configure the 2nd SOAM server, repeat steps 1 through 7 for 2nd SOAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td><strong>Insert and Configure the 2nd SOAM server, repeat steps 1 through 7 for 2nd SOAM</strong></td>
</tr>
<tr>
<td></td>
<td>1. Repeat this procedure to insert and configure the 2nd SOAM server, with the exception of the NTP server, which should be configured as so:</td>
</tr>
<tr>
<td></td>
<td>Enter the network data for the 2nd SOAM server, transfer the <strong>TKLCConfigData</strong> file to the 2nd SOAM server, and reboot the 2nd SOAM server when asked at a terminal window.</td>
</tr>
<tr>
<td></td>
<td>2. Wait approximately 5 minutes for the 2nd SOAM server to reboot.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For DSR mated sites, repeat this step for additional/spare SOAM server for mated site.</td>
</tr>
</tbody>
</table>
Procedure 19. Configure the SOAM Server Group

This procedure configures the SOAM server group.
Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Primary NOAM VIP GUI: Enter SOAM server group data</td>
</tr>
<tr>
<td>1.</td>
<td>From the GUI session on the NOAM VIP address, navigate to <strong>Main Menu- &gt;Configuration-&gt;Networking-&gt;Server Groups.</strong></td>
</tr>
<tr>
<td></td>
<td>Click <strong>Insert</strong> and add the SOAM server group name along with the values for the following fields:</td>
</tr>
<tr>
<td></td>
<td>Name: [Enter Server Group Name]</td>
</tr>
<tr>
<td></td>
<td>Level: B</td>
</tr>
<tr>
<td></td>
<td>Parent: [Select the NOAM Server Group]</td>
</tr>
<tr>
<td></td>
<td>Function: <strong>DSR (Active/Standby Pair)</strong></td>
</tr>
<tr>
<td></td>
<td>WAN Replication Connection Count: Use Default Value</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>OK</strong> when all fields are filled.</td>
</tr>
<tr>
<td>Note:</td>
<td>For DSR mated sites, repeat this step for additional SOAM server groups where the preferred SOAM spares may be entered before the active/standby SOAMs.</td>
</tr>
</tbody>
</table>
Procedure 19. Configure the SOAM Server Group


2. Select the new SOAM server group and click Edit.

<table>
<thead>
<tr>
<th>Server</th>
<th>SG Inclusion</th>
<th>Preferred HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>S01</td>
<td>Include in SG</td>
<td></td>
</tr>
<tr>
<td>S02</td>
<td>Include in SG</td>
<td></td>
</tr>
</tbody>
</table>

3. Add both SOAM servers to the server group primary site by marking the Include in SG checkbox.

4. Click Apply.
Procedure 19. Configure the SOAM Server Group


2. Select the new SOAM server group and click Edit.

3. Click Add to add a SOAM VIP. Type the VIP Address and click OK.

4. If the two-site redundancy feature is wanted for the SOAM server group, add an SOAM server located in its server group secondary site by marking the Include in SG and Preferred Spare checkboxes.

5. Additional SOAM VIPs only apply to SOAM server groups with preferred spare SOAMs.
### Procedure 19. Configure the SOAM Server Group

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6.</strong></td>
<td><strong>Primary NOAM VIP GUI:</strong> Wait for replication&lt;br&gt;After replication, the server status should be active ((\text{Main Menu}\rightarrow\text{Status &amp; Manage}\rightarrow\text{HA})).&lt;br&gt;<strong>Note:</strong> This may take up to 5 minutes while the servers figure out master/slave relationship.&lt;br&gt;Look for the alarm ID 10200 &quot;Remote Database re-initialization in progress&quot; to be cleared before proceeding ((\text{Main Menu}\rightarrow\text{Alarms}\rightarrow\text{View Active})).</td>
</tr>
<tr>
<td><strong>7.</strong></td>
<td><strong>Primary NOAM VIP GUI:</strong> Restart 1st SOAM server&lt;br&gt;1. From the NOAM GUI, navigate to <strong>Main Menu</strong>(\rightarrow\text{Status &amp; Manage}\rightarrow\text{Server}** and select the 1st SOAM server.&lt;br&gt;2. Click <strong>Restart</strong>.&lt;br&gt;3. Click <strong>OK</strong> on the confirmation screen.&lt;br&gt;Wait for restart to complete. Wait for the Appl State to change to Enabled, and all other columns to Norm.</td>
</tr>
<tr>
<td><strong>8.</strong></td>
<td><strong>Primary NOAM VIP GUI:</strong> Restart 2nd SOAM server&lt;br&gt;Repeat step 7 for the second SOAM.</td>
</tr>
<tr>
<td><strong>9.</strong></td>
<td><strong>Primary NOAM VIP GUI:</strong> Restart all preferred spare SOAM servers (Optional)&lt;br&gt;1. If additional preferred spare servers are configured for secondary sites, navigate to <strong>Main Menu</strong>(\rightarrow\text{Status &amp; Manage}\rightarrow\text{Server}** and select all <strong>Preferred Spare</strong> SOAM servers.&lt;br&gt;2. Click <strong>Restart</strong>. Click <strong>OK</strong> to the confirmation popup. Wait for the Appl State to change to <strong>Enabled</strong> and all other columns to change to <strong>Norm</strong>.</td>
</tr>
</tbody>
</table>
### Procedure 20. Activate PCA/DCA (PCA/DCA Only)

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. (PCA Only)</td>
<td><strong>Activate PCA feature</strong>&lt;br&gt;If you are installing PCA, execute the applicable procedures (Added SOAM site activation or complete system activation) of the DSR PCA Activation Guide [2] to activate PCA.&lt;br&gt;&lt;br&gt;<em>Note:</em> If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online.&lt;br&gt;&lt;br&gt;<em>Note:</em> Ignore steps to restart DA-MPs and SBRs that have yet to be configured.</td>
</tr>
<tr>
<td>2. (DCA Only)</td>
<td><strong>Activate DCA feature</strong>&lt;br&gt;If you are installing PCA, execute [24] DCA Framework and Application Activation and Deactivation Guide to activate the DCA framework and feature.&lt;br&gt;&lt;br&gt;<em>Note:</em> If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online.&lt;br&gt;&lt;br&gt;<em>Note:</em> Ignore steps to restart DA-MPs and SBRs that have yet to be configured.</td>
</tr>
</tbody>
</table>

### Procedure 21. Configure the MP Virtual Machines

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Primary NOAM VIP GUI: Establish GUI Session on the NOAM VIP</td>
<td>1. If needed, establish a GUI session on the NOAM by using the NOAM VIP address.&lt;br&gt;2. Login as the <strong>guiadmin</strong> user.</td>
</tr>
</tbody>
</table>
Procedure 21. Configure the MP Virtual Machines

1. Navigate to Main Menu->Configuration->Networking->Networks.

2. Navigate to the SO Network Element tab under which the MPs are to be configured.

3. **Primary NOAM VIP GUI:** Add signaling networks

The following screen displays:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>X012</td>
<td>The name of this network. [Default = NA, Range = Alphanumeric, 1-255 chars, starting with a letter; A value is required]</td>
</tr>
<tr>
<td>Network Type</td>
<td>Signaling</td>
<td>The type of this network.</td>
</tr>
<tr>
<td>VLAN ID *</td>
<td>7</td>
<td>The VLAN ID to use for this network. [Default = NA, Range = 1-4096] [A value is required]</td>
</tr>
<tr>
<td>Network Address</td>
<td>10.195.225.0</td>
<td>The network address of this network. [Default = NA, Range = Valid IPv4 or IPv6 address]</td>
</tr>
<tr>
<td>Netmask *</td>
<td>255.255.255.0</td>
<td>Subnetting to apply to devices within this network. [Default = NA, Range = 255.0.0.0 - 255.255.255.255]</td>
</tr>
<tr>
<td>Router IP</td>
<td></td>
<td>The IP address of a router on this network. If this is a default network, this value is the gateway address of the default route and is enabled, this address will be used. [Default = NA, Range = Valid IPv4 or IPv6]</td>
</tr>
<tr>
<td>Default Network</td>
<td>Yes</td>
<td>A selection indicating whether this is a default gateway.</td>
</tr>
<tr>
<td>Routable</td>
<td>Yes</td>
<td>Whether or not this network is routed outside its network element. If it is not assigned to a network element, it is assumed to be possible.</td>
</tr>
</tbody>
</table>

1. Type the **Network Name**, **Network Type**, **VLAN ID**, **Network Address**, **Netmask**, and **Router IP** that matches the signaling network.

   **Note:** Even if the network does not use VLAN tagging, you should type the correct VLAN ID here as indicated by the NAPD.

   a. Select **Signaling** for Network Type.
   b. Select **No** for Default Network.
   c. Select **Yes** for Routable.

2. Click **OK** if you are finished adding signaling networks

   **-OR-**
   Click **Apply** to save this signaling network and repeat this step to enter additional signaling networks.
Procedure 21. Configure the MP Virtual Machines

4. **Primary NOAM VIP GUI:** (PCA/DCA only) Navigate to signaling network configuration screen

   **Note:** Execute this step only if you are defining a separate, dedicated network for SBR Replication.

   1. Navigate to **Main Menu->Configuration->Networking->Networks.**

   - **Main Menu**
     - Administration
     - Configuration
     - Networking
     - Devices

   2. Click **Insert** in the lower left corner.

   ![Networks Screen](image)

   **Note:** Execute this step only if you are defining a separate, dedicated network for SBR replication.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name</td>
<td>Replication</td>
<td>The name of this network. [Default = NA. Range = Alphanumeric string up to 81 characters, starting with a letter]</td>
</tr>
<tr>
<td>Network Type</td>
<td>Signaling</td>
<td>The type of this network.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>0</td>
<td>The VLAN ID to use for this network. [Default = NA. Range = 1-4094]</td>
</tr>
<tr>
<td>Network Address</td>
<td>10.136.234.1</td>
<td>The network address of this network. [Default = NA. Range = Valid Network Address of the network in dotted]</td>
</tr>
<tr>
<td>Netmask</td>
<td>255.255.255.0</td>
<td>Subnetting to apply to servers within this network. [Default = NA. Range = Valid Netmask for the networking]</td>
</tr>
<tr>
<td>Router IP</td>
<td></td>
<td>The IP address of a router on this network. If this is a default network, this will be used as the gateway address enabled, this address will be the one monitored.</td>
</tr>
<tr>
<td>Default Network</td>
<td>No</td>
<td>A selection indicating whether this is the network with a default gateway.</td>
</tr>
<tr>
<td>Routable</td>
<td>Yes</td>
<td>Whether or not this network is routed outside this network element. If it is not assigned to a network element, it will be considered by the NAPD as belonging to a default network.</td>
</tr>
</tbody>
</table>

   1. Type the **Network Name**, **Network Type**, **VLAN ID**, **Network Address**, **Netmask**, and **Router IP** that matches the SBR DB replication network.

   **Note:** Even if the network does not use VLAN tagging, you should type the correct VLAN ID here as indicated by the NAPD.

   a. Select **No** for Default Network.
   b. Select **Yes** for Routable.

   2. Click **OK** if you are finished adding signaling networks.

   **-OR-**

   Click **Apply** to save this signaling network and repeat this step to enter additional signaling networks.

   **Note:** Execute this step only if you are defining a separate, dedicated network for SBR replication.

5. **Primary NOAM VIP GUI:** (PCA only) Define SBR DB replication network

6. **Primary NOAM VIP GUI:** (PCA only) Perform
Procedure 21. Configure the MP Virtual Machines


   Navigate to Main Menu>
   Administration>
   Configuration>
   Networking>
   Networks>
   Devices>
   Routes>
   Services>
   Servers>
   Server Groups>
   Resource Domains

   Click Edit.

   ![](Edit.png)

   ![](Report.png)

2. Set the services using one of the following scenarios:
   - **If the dual-path HA configuration is required**:
     
     For HA_MP_Secondary, Oracle recommends the inter-NE network is set as the XMI network and intra-NE network is set as the IMI network. If the primary interface (Replication_MP) SBR DB Replication Network interface goes down, use the secondary network for sharing HA status to reduce the likelihood of a split brain. This leads to DSR mate isolation from the active SBR and results in traffic loss until SBR DB Replication Network is down.

     | Name             | Intra-NE Network | Inter-NE Network |
     |------------------|------------------|-----------------|
     | HA_MP_Secondary  | <IMI Network>    | <XMI Network>   |
     | Replication_MP   | <IMI Network>    | <SBR DB Replication Network> |
     | ComAgent         | <IMI Network>    | <SBR DB Replication Network> |

   - **If the dual-path HA configuration is NOT required**:  
     
     The intra-NE network is set as the IMI network and inter-NE network is set as the PCA replication network (configured in step 5). This may lead to a split database scenario in case the SBR DB Replication Network interface goes down. Due to this, an active SBR server in each site is in effect.
### Procedure 21. Configure the MP Virtual Machines

<table>
<thead>
<tr>
<th>Name</th>
<th>Intra-NE Network</th>
<th>Inter-NE Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>HA_MP_Secondary</td>
<td>&lt;IMI Network&gt;</td>
<td>&lt;SBR DB Replication Network&gt;</td>
</tr>
<tr>
<td>Replication_MP</td>
<td>&lt;IMI Network&gt;</td>
<td>&lt;SBR DB Replication Network&gt;</td>
</tr>
<tr>
<td>ComAgent</td>
<td>&lt;IMI Network&gt;</td>
<td>&lt;SBR DB Replication Network&gt;</td>
</tr>
</tbody>
</table>

3. Click **OK** to apply the Service-to-Network selections.

#### 7. Primary NOAM VIP GUI: Insert the MP or IPFE server – Part 1

1. Navigate to **Main Menu->Configuration->Networking->Servers.**

2. Click **Insert** to add the new MP or IPFE server into servers table.

3. Fill in the following values:
Procedure 21. Configure the MP Virtual Machines

Fill in the fields as follows:

4. **Hostname:** <Hostname>  
   **Role:** MP  
   **System ID:** <Site System ID>  
   **Hardware Profile:** DSR Guest  
   **Network Element Name:** [Choose NE from list]

<table>
<thead>
<tr>
<th>Network</th>
<th>IP Address</th>
<th>Interface</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNALXMI (10.196.227.0/24)</td>
<td>10.196.227.0</td>
<td>eth0</td>
<td>VLAN(6)</td>
</tr>
<tr>
<td>INTERNALMI (10.254.1.0/24)</td>
<td>169.254.1.0</td>
<td>eth0</td>
<td>VLAN(5)</td>
</tr>
<tr>
<td>XSI1 (10.196.228.0/25)</td>
<td>10.196.228.0</td>
<td>eth0</td>
<td>VLAN(26)</td>
</tr>
<tr>
<td>XSI2 (10.196.120.0/25)</td>
<td>10.196.120.0</td>
<td>eth0</td>
<td>VLAN(27)</td>
</tr>
</tbody>
</table>

5. For the XMI network, type the MP's XMI IP address. Select the correct interface.

6. Leave the **VLAN** checkbox unmarked.

7. For the IMI network, type the MP's IMI **IP address**. Select the correct interface.
**Procedure 21. Configure the MP Virtual Machines**

- a. Leave the VLAN checkbox unmark.
- b. For the Replication network, type the MP's XSI2 IP address. Select the correct interface. Leave the VLAN checkbox unmarked.

8. For the XSI1 network, type the MP's XSI1 IP address. Select the correct interface.
   - a. Leave the VLAN checkbox unmark.

9. For the XSI2 network, type the MP's XSI2 IP address. Select the correct interface.
   - a. Leave the VLAN checkbox unmark.
   
   **Note:** If more XSI networks are configured, follow the same method of entry as XSI1 and XSI2. All interfaces need to be added sequentially for any server.

10. Add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid NTP server</td>
<td>Yes</td>
</tr>
<tr>
<td>Valid NTP server</td>
<td>No</td>
</tr>
<tr>
<td>Valid NTP server</td>
<td>No</td>
</tr>
</tbody>
</table>

11. Click OK when all fields are filled in to finish MP server insertion.

---

**8. Primary NOAM VIP GUI: Export the initial configuration**

1. Navigate to **Main Menu->Configuration->Networking-> Servers**.

2. From the GUI screen, select the server that was just configured and click **Export** to generate the initial configuration data for that server.

3. Go to the Info tab to confirm the file has been created.

---

**9. MP Server: Log into the MP**

---

**10. Primary NOAM VIP GUI: Copy configuration file to MP or IPFE server**

From the active NOAM console, login as the admusr user.

```
$ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh
```

**Note:** ipaddr is the XMI IP address of the MP or IPFE.
## Procedure 21. Configure the MP Virtual Machines

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
</table>
| 11. | **MP Server:** Wait for configuration to complete | 1. Obtain a terminal session on the **MP or IPFE** as the **admusr** user. The automatic configuration daemon looks for the file named **TKLCConfigData.sh** in the **/var/tmp** directory, implements the configuration in the file, and prompts the user to reboot the server.  
2. If you are on the console, wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure.  
3. Verify script completed successfully by checking the following file. $ sudo cat /var/TKLC/appw/logs/Process/install.log  
   **Note:** Ignore the warning about removing the USB key since no USB key is present. |
| 12. | **MP Server:** Reboot the server | Obtain a terminal session on the **MP or IPFE** as the **admusr** user. $ sudo init 6  
   Wait for server to reboot.  
1. After the reboot, login as the **admusr** user.  
2. Execute the following command as super-user on the server and make sure that no errors are returned: $ sudo syscheck  
   Running modules in class hardware...  
      OK  
   Running modules in class disk...  
      OK  
   Running modules in class net...  
      OK  
   Running modules in class system...  
      OK  
   Running modules in class proc...  
      OK  
   LOG LOCATION: /var/TKLC/log/syscheck/fail_log |
| 13. | **MP Server:** Verify server health |  
1. Log into the **MP** as the **admusr** user. (Alternatively, you can log into the VM’s console.)  
2. Determine **<XMI_Gateway_IP>** from your SO site network element information.  
3. Gather the following items: |
| 14. | **MP Server:** Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network (Optional) | **Note:** THIS STEP IS OPTIONAL AND SHOULD ONLY BE EXECUTED IF YOU PLAN TO CONFIGURE A DEFAULT ROUTE ON YOUR MP THAT USES A SIGNALING (XSI) NETWORK INSTEAD OF THE XMI NETWORK. Not executing this step means a default route is not configurable on this MP and you have to create separate network routes for each signaling network destination.  
1. Log into the MP as the **admusr** user.  
2. Determine **<XMI_Gateway_IP>** from your SO site network element information.  
3. Gather the following items:
Procedure 21. Configure the MP Virtual Machines

<NO_XMI_Network_Address>
<NO_XMI_Network_Netmask>

**Note:** You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the **Main Menu->Configuration->Networking->Networks** menu.

4. Create network routes to the NO’s XMI (OAM) network:
   a. Navigate to NOAM VIP GUI **Configuration->Networking->Routes**.
   b. Select the Specific MP.
   c. Click **Insert**.
   d. Enter details.
   e. Click **OK**.

5. (Optional) [MP console] If sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network:

   `$ sudo /usr/TKLC/plat/bin/netAdm add --route=host --address=<Customer_NMS_IP> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface>

   Route to <MP_XMI_Interface> added.

6. Route to <MP_XMI_Interface> added.

7. Repeat for any existing customer NMS stations.

8. Delete the existing default route:

   `$ sudo /usr/TKLC/plat/bin/netAdm delete --route=default --gateway=<MP_XMI_Gateway_IP> --device=<MP_XMI_Interface>

   Route to <MP_XMI_Interface> removed.`
### Procedure 21. Configure the MP Virtual Machines

9. [MP Console] Ping active NO XMI IP address to verify connectivity:
   ```
   $ ping <ACTIVE_NO_XMI_IP_Address>
   PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.
   64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms
   64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms
   ```

10. (Optional) [MP Console] Ping Customer NMS Station(s):
    ```
    $ ping <Customer_NMS_IP>
    PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data.
    64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms
    64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms
    ```

11. If you do not get a response, then verify your network configuration. If you continue to get failures then halt the installation and contact Oracle customer support.

15. Repeat for remaining MPs and IPFEs

### Repeat steps 7 through 14 for all remaining MP (SBR, SS7-MP, DA-MP, IPFE and vSTP) servers.

### Procedure 22. Configure the MP Virtual Machines (Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>This procedure configures MP VMs (IPFE, SBR, SS7-MP, DA-MP, and vSTP).</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Note:</strong> This procedure is ONLY required if additional MPs are required to be added to expand an existing DSR, which was upgraded from 7.x to 8.x.</td>
</tr>
<tr>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STEP #</th>
<th>PRIMARY NOAM VIP GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Establish GUI Session on the NOAM VIP</td>
</tr>
<tr>
<td></td>
<td>Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the <strong>guiadmin</strong> user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STEP #</th>
<th>PRIMARY NOAM VIP GUI:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Insert the MP or IPFE server – Part 1</td>
</tr>
<tr>
<td>1.</td>
<td>Navigate to <strong>Main Menu-&gt;Configuration-&gt;Networking-&gt;Servers</strong>.</td>
</tr>
</tbody>
</table>
**Procedure 22. Configure the MP Virtual Machines (Optional)**

2. Click **Insert** to add the new MP or IPFE server into servers table.

3. Fill in the following values:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>&lt;Hostname&gt;</td>
</tr>
<tr>
<td>Role</td>
<td>- Select Role -</td>
</tr>
<tr>
<td>System ID</td>
<td></td>
</tr>
<tr>
<td>Hardware Profile</td>
<td>DSR Guest</td>
</tr>
<tr>
<td>Network Element Name</td>
<td>- Unassigned -</td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
</tbody>
</table>

4. Fill in the fields as follows:

  - Hostname: `<Hostname>`
  - Role: `MP`
  - System ID: `<Site System ID>`
  - Hardware Profile: `DSR Guest`
  - Network Element Name: `[Choose NE from list]`
Procedure 22. Configure the MP Virtual Machines (Optional)

<table>
<thead>
<tr>
<th>Network</th>
<th>IP Address</th>
<th>Interface</th>
<th>VLAN (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTERNAL XMI</td>
<td>10.196.227.1</td>
<td>eth0</td>
<td></td>
</tr>
<tr>
<td>INTERNAL IMI</td>
<td>169.254.1.024</td>
<td>eth0</td>
<td>VLAN (3)</td>
</tr>
</tbody>
</table>

5. For the XMI network, type the MP's XMI IP address. Select the correct interface.
   Leave the VLAN checkbox unmarked.

6. For the IMI network, type the MP's IMI IP address. Select the correct interface.
   Leave the VLAN checkbox unmarked.

7. Add the following NTP servers:

<table>
<thead>
<tr>
<th>NTP Server</th>
<th>Preferred?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid NTP server Yes</td>
<td></td>
</tr>
<tr>
<td>Valid NTP server No</td>
<td></td>
</tr>
<tr>
<td>Valid NTP server No</td>
<td></td>
</tr>
</tbody>
</table>

8. Click OK when all fields are filled in to finish MP server insertion.


   2. From the GUI screen, select the server that was just configured and click Export to generate the initial configuration data for that server.

3. Go to the Info tab to confirm the file has been created.

   Obtain a terminal window connection on the MP or IPFE server.

4. Primary NOAM VIP GUI: Log into the MP

5. Primary NOAM VIP Server: Copy configuration file to MP or IPFE server

   From the active NOAM console, login as the admusr user.
   
   $ sudo scp 
   /var/TKLCLC/db/filemgmt/TKLCLCConfigData.<hostname>.sh 
   admusr@<ipaddr>:/var/tmp/TKLCLCConfigData.sh 

   Note: ipaddr is the XMI IP address of the MP or IPFE.
**Procedure 22. Configure the MP Virtual Machines (Optional)**

<table>
<thead>
<tr>
<th></th>
<th>MP Server</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td><strong>Wait for configuration to complete</strong></td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td><strong>Reboot the server</strong></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td><strong>Verify server health</strong></td>
<td></td>
</tr>
<tr>
<td>9.</td>
<td><strong>Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network (Optional)</strong></td>
<td></td>
</tr>
</tbody>
</table>

1. Obtain a terminal session on the **MP or IPFE** as the **admusr** user.
   - The automatic configuration daemon looks for the file named `TKLCCfgData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.
   - If you are on the console, wait to be prompted to reboot the server, but **DO NOT** reboot the server, it is rebooted later in this procedure.
   - Verify script completed successfully by checking the following file.
     ```
     $ sudo cat /var/TKLC/appw/logs/Process/install.log
     ```
   - **Note:** Ignore the warning about removing the USB key since no USB key is present.

2. Obtain a terminal session on the **MP or IPFE** as the **admusr** user.
   - `$ sudo init 6`
   - Wait for server to reboot.
   - **Note:** **THIS STEP IS OPTIONAL AND SHOULD ONLY BE EXECUTED IF YOU PLAN TO CONFIGURE A DEFAULT ROUTE ON YOUR MP THAT USES A SIGNALING (XSI) NETWORK INSTEAD OF THE XMI NETWORK.** Not executing this step means a default route is not configurable on this MP and you have to create separate network routes for each signaling network destination.
   - Log into the MP as the **admusr** user. (Alternatively, you can log into the VM’s console.)
   - Determine `<XMI_Gateway_IP>` from your SO site network element information.
   - Gather the following items:
Procedure 22. Configure the MP Virtual Machines (Optional)

<NO_XMI_Network_Address>
<NO_XMI_Network_Netmask>

**Note:** You can either consult the XML files you imported earlier, or go to the NO GUI and view these values from the **Main Menu->Configuration->Networking->Networks** menu.

4. Create network routes to the NO’s XMI (OAM) network:
   a. Navigate to NOAM VIP GUI **Configuration->Networking->Routes**.
   b. Select the Specific MP.
   c. Click **Insert**.
   d. Enter details.
   e. Click **OK**.

5. (Optional) [MP console] If sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network:

   $ sudo /usr/TKLC/plat/bin/netAdm add --route=host
   --address=<Customer_NMS_IP>
   --gateway=<MP_XMI_Gateway_IP_Address>
   --device=<MP_XMI_Interface>

   Route to <MP_XMI_Interface> added.

6. Route to <MP_XMI_Interface> removed.

7. Repeat for any existing customer NMS stations.

8. Delete the existing default route:

   $ sudo /usr/TKLC/plat/bin/netAdm delete --route=default --gateway=<MP_XMI_Gateway_IP> --device=<MP_XMI_Interface>

   Route to <MP_XMI_Interface> removed.
### Procedure 22. Configure the MP Virtual Machines (Optional)

<table>
<thead>
<tr>
<th></th>
<th>Procedure</th>
</tr>
</thead>
</table>
| 9. | [MP Console] Ping active NO XMI IP address to verify connectivity:  
    | $ ping <ACTIVE_NO_XMI_IP_Address>  
    | PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.  
    | 64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms  
    | 64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms |
| 10. | (Optional) [MP Console] Ping Customer NMS Station(s):  
    | $ ping <Customer_NMS_IP>  
    | PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data.  
    | 64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms  
    | 64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms |
| 11. | If you do not get a response, then verify your network configuration. If you continue to get failures then halt the installation and contact Oracle customer support. |

Repeat steps 2 through 9 for all remaining newly created MPs.
### Procedure 23. Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only)

This procedure adds places in the MAP-IWF and PCA network. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>(PCA Only) Primary NOAM VIP GUI: Configure Places</td>
</tr>
</tbody>
</table>

1. Establish a GUI session on the NOAM by using the XMI VIP address. Login as the guiadmin user.

2. Navigate to **Main Menu->Configuration->Networking->Places**.

3. Click **Insert**.

4. Fill in the fields as follows:

   **Inserting a new Place**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Place Name</td>
<td>&lt;Site Name&gt;</td>
<td>Unique identifier used to label a Place [Def: and space] [A value is required.]</td>
</tr>
<tr>
<td>Parent</td>
<td>NONE</td>
<td>The Parent of this Place [A value is required.]</td>
</tr>
<tr>
<td>Place Type</td>
<td>Site</td>
<td>The Type of this Place [A value is required.]</td>
</tr>
</tbody>
</table>

5. Repeat this step for each of the PCA/DCA Places (Sites) in the network. See the Terminology section for more information on Sites & Places.
Procedure 23. Configure Places and Assign MP Servers to Places (MAP-IWF, PCA and DCA Only)

2. NOAM VIP GUI: Assign MP server to places

   1. Select the place configured in step 1 and click Edit.

```
Editing Place ZombiePlace

Place Type: Site

Servers

- ZombieNOAM
  - ZombieNOAM1
  - ZombieNOAM2
- ZombieDRNOAM
  - ZombieDRNOAM1
  - ZombieDRNOAM2
- ZombieSOAM
  - ZombieSOAM1
  - ZombieSOAM2
  - ZombieDAMPSBR

Ok Apply Cancel
```

2. Mark all the checkboxes for SS7-MPs and PCA/DCA DA-MP and SBR servers that are assigned to this place.

3. Repeat this step for all other DA-MP or SBR servers you wish to assign to places.

**Note:** All DA-MPs and SBR servers must be added to the Site Place that corresponds to the physical location of the server. See the Terminology section for more information on Sites & Places.

Procedure 24. Configure the MP Server Group(s) and Profiles

1. Primary NOAM VIP GUI: Enter MP or IPFE Server Group Data

```
1. From the GUI session on the NOAM VIP address, navigate to Main Menu->Configuration->Networking->Server Groups.
```
Procedure 24. Configure the MP Server Group(s) and Profiles

2. Click **Insert** and fill out the following fields:

   - **Server Group Name:** [Server Group Name]
   - **Level:** C
   - **Parent:** [SOAM Server Group That is Parent To this MP]
   - **Function:** Select the Proper Function for this MP Server Group:

<table>
<thead>
<tr>
<th>Server Group Function</th>
<th>MPs Will Run</th>
<th>Redundancy Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSR (multi-active cluster)</td>
<td>Diameter Relay and Application Services</td>
<td>Multiple MPs Active per SG</td>
</tr>
<tr>
<td>DSR (active-standby pair)</td>
<td>Diameter Relay and Application Services</td>
<td>1 Active MP and 1 Standby MP/Per SG</td>
</tr>
<tr>
<td>IP Front End</td>
<td>IPFE application</td>
<td>1 Active MP Per SG</td>
</tr>
<tr>
<td>SBR</td>
<td>Policy and Charging Session/or Policy Binding Function/Universal SBR</td>
<td>1 Active MP, 1 Standby MP, 2 Optional Spare Per SG</td>
</tr>
<tr>
<td>SS7-IWF</td>
<td>MAP IWF Application</td>
<td>1 Active MP per SG</td>
</tr>
<tr>
<td>STP</td>
<td>vSTP</td>
<td>1 vSTP MP per SG</td>
</tr>
</tbody>
</table>

**For vSTP:**

If configuring only vSTP application, ignore all other MP/IPFE configuration. Currently, there is no specific MP profile for vSTP MP.

**Note:** When vSTP co-exists with DA-MP, there will be a major alarm regarding ‘Communication Agent Connection Down’ which can be ignored.

**For PCA application:**

- Online Charging function (only)
  
  At least one MP Server Group with the **SBR** function must be configured.
  
  At least one MP Server Group with the **DSR (multi-active cluster)** function must be configured.

- Policy DRA function
  
  At least two MP Server Groups with the **SBR** function must be configured. One stores session data and one stores binding data.
Procedure 24. Configure the MP Server Group(s) and Profiles

At least one MP Server Group with the **DSR (multi-active cluster)** function must be configured.

**WAN Replication Connection Count:**

- For non-Policy and Charging SBR Server Groups: **Default Value**
- For Policy and Charging Server Groups: **8**

For the PCA application, the following types of MP Server Groups must be configured:

- DA-MP (Function: DSR (multi-active cluster))
- SBR (Function: SBR)
- IPFE (Function: IP Front End)

3. Click **OK** when all fields are filled in.

Repeat step 1 for any remaining MP and IPFE server groups you wish to create. For instance, when installing an IPFE, you need to create an IP front end server group for each IPFE server.

- **Primary NOAM VIP GUI:** Repeat for additional server groups
- **Primary NOAM VIP GUI:** Edit the MP server groups to include MPs

1. Navigate to **Main Menu->Configuration->Networking->Server Groups**, select a server group that you just created, and click **Edit**.

2. Select the network element representing the MP server group you wish to edit.

3. Mark the **Include in SG** checkbox for every MP server you wish to include in this server group. Leave other checkboxes blank.

<table>
<thead>
<tr>
<th>Server</th>
<th>SG Inclusion</th>
<th>Preferred HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAMP1</td>
<td>✓ Include in SG</td>
<td></td>
</tr>
<tr>
<td>DAMP2</td>
<td>✓ Include in SG</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Each IPFE, SS7-MP and vSTP-MP server should be in its own server group.

4. Click **OK**.
**Procedure 24. Configure the MP Server Group(s) and Profiles**

4. **Primary NOAM VIP GUI:** (PCA only) Edit the MP server group and add preferred spares for site redundancy (Optional)

   If two-site redundancy for the Policy and Charging SBR Server Group is wanted, add a MP server that is physically located in a separate site(location) to the server group by marking the **Include in SG** checkbox and also mark the **Preferred Spare** checkbox.

<table>
<thead>
<tr>
<th>Server</th>
<th>SG Inclusion</th>
<th>Preferred HA Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBR1</td>
<td>✅ Include in SG</td>
<td>✅ Prefer server as spare</td>
</tr>
</tbody>
</table>

   If three-site redundancy for the SBR MP server group is wanted, add two SBR MP servers that are both physically located in separate sites (location) to the server group by marking the **Include in SG** and **Preferred Spare** checkboxes for both servers.

   **Note:** The preferred spare servers should be different sites from the original server. There should be servers from three separate sites (locations).

   **Note:** There must first be non-preferred spare present in the server group before adding the preferred spare.

   For more information about site redundancy for Policy and Charging SBR Server Groups, see the **Terminology** section.

   Click **OK** to save.

5. **Primary NOAM VIP GUI:** Repeat For additional server groups

   Repeat steps 1 through 4 for any remaining MP and IPFE server groups you need to create.

6. **Primary NOAM VIP GUI:** Wait for replication to complete on all MPs

   Wait for the alarm “10200: Remote Database re-initialization in progress” to be cleared (Main Menu->Alarms & Events->Active Alarms).

   ![View Active](image1)
   ![View History](image2)
   ![View Trap Log](image3)

   This should happen shortly after you have verified the **Norm** DB status in the previous step.
Procedure 24. Configure the MP Server Group(s) and Profiles

1. Log into the GUI of the active SOAM server as the guiadmin user.
2. From the SO GUI, navigate to Main Menu->Diameter Common->MPs->Profiles Assignments.

   SOAM VIP GUI:
   Assign profiles to DA-MPs from SOAM GUI

   Log into the GUI of the active SOAM server as the guiadmin user.
   1. From the SO GUI, navigate to Main Menu->Diameter Common->MPs->Profiles Assignments.

   Refer to the DA-MP section. If the site has both DSR and MAP-IWF server groups, you see both DA-MP and SS7-MP sections.

<table>
<thead>
<tr>
<th>DA-MP</th>
<th>MP Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA1</td>
<td>VM:30K_MPS</td>
</tr>
</tbody>
</table>

   3. For each MP, select the proper profile assignment based on the MP’s type and the function it serves:

   VM:10K_MPS
   VM:6K_MPS
   VM:8K_MPS
   VM:12K_MPS
   VM:14K_MPS
   VM:16K_MPS
   VM:18K_MPS
   VM:21K_MPS
   VM:24K_MPS
   VM:27K_MPS
   VM:30K_MPS

   **Note:** If the DA-MPs at this site are configured for Active/Standby then there is a single selection box visible that assigns profiles for all MPs.

   4. When finished, click Assign.
**Procedure 24. Configure the MP Server Group(s) and Profiles**

### SOAM VIP GUI: Assign Profiles to SS7-MPs from SOAM GUI

1. Log into the GUI of the active SOAM server as the **guiadmin** user.
2. From the SO GUI, navigate to **Main Menu->Diameter->Configuration->MPs->Profiles Assignments**.

![Diameter Common]
- Dashboard
- Network Identifiers
- MPGroups
  - Profiles
  - Profile Assignments

Refer to the **SS7-MP** section. If the site has both DSR and MAP-IWF server groups, you see both DA-MP and SS7-MP sections.

<table>
<thead>
<tr>
<th>SS7-MP</th>
<th>MP Profile</th>
<th>current value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS7MP2</td>
<td>VM:MD-IWF</td>
<td>The current MP Profile for SS7MP2 is VM:MD-IWF. Virtualized SS7-MP running MD-IWF application if required.</td>
</tr>
</tbody>
</table>

3. For each SS7 MP, select the proper profile assignment based on the SS7 MP’s type and the function it serves:

<table>
<thead>
<tr>
<th>Profile Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM:MD-IWF</td>
<td>VM Running MAP-IWF functions</td>
</tr>
</tbody>
</table>

4. When finished, click **Assign**.

### Primary NOAM VIP GUI: Restart MP VM

1. From the NOAM GUI, navigate to **Main Menu->Status & Manage->Server**.

![Status & Manage]
- Network Elements
- Server
- HA
- Database
- KPIs
- Processes

2. For each MP server:
   a. Select the MP server.
   b. Click **Restart**.
   c. Click **OK** on the confirmation screen. Wait for the message that tells you that the restart was successful.

**Policy and Charging DRA/DCA Installations**: You may continue to see alarms related to ComAgent until you complete PCA/DCA installation.
4.6 Configure Signaling Devices (Optional)

Procedure 25. Configure the Signaling Devices (Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Newly created MP Server console</strong>: Manually configure signaling interface</td>
</tr>
</tbody>
</table>
|        | 1. SSH into the newly added MP  
$ ssh admusr@<XMI_Interface_Of_Neulessly_Created_MP>  
2. Configure the signaling network interfaces, conforming the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.  
   $ sudo netAdm add --onboot=yes --bootproto=none --device=eth2 --address=<xsi1 ip> --netmask=<xsi1 net mask>  
   $ sudo netAdm add --onboot=yes --bootproto=none --device=eth3 --address=<xsi2 ip> --netmask=<xsi2 net mask>  
   Repeat the above netAdm commands to configure the required number of the Signaling network interfaces.  
3. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebootsing.  
   $ sudo init 6 |

**Note**: This procedure is ONLY required if additional MPs need to be added to expand an existing DSR, which was upgraded from 7.x to 8.x.

**Prerequisite**: Execute Procedure 22.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
### Procedure 25. Configure the Signaling Devices (Optional)

1. Navigate to **Main Menu->Configuration->Networking-> Devices.**

   - **Configuration**
     - **Networking**
       - **Devices**
     - **Routers**
     - **Services**

2. You should see several tabs each representing a server in the system. Click on the tab representing the newly created MP.

   ![Server tabs](image)

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device Type</th>
<th>Device Options</th>
<th>IP Interface (Network)</th>
<th>Configuration Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>eth1</td>
<td>Ethernet</td>
<td>MTU = 1500</td>
<td>192.168.2.240</td>
<td>Deployed</td>
</tr>
<tr>
<td>eth2</td>
<td>Ethernet</td>
<td>MTU = 1500</td>
<td>192.168.2.241</td>
<td>Deployed</td>
</tr>
<tr>
<td>eth3</td>
<td>Ethernet</td>
<td>MTU = 1500</td>
<td>192.168.2.242</td>
<td>Deployed</td>
</tr>
<tr>
<td>eth4</td>
<td>Ethernet</td>
<td>MTU = 1500</td>
<td>192.168.2.243</td>
<td>Deployed</td>
</tr>
</tbody>
</table>

3. Select all newly configured Signaling Ethernet devices that have **Discovered** as their Configuration Status.

   ![Discovered devices](image)

   **Click Take Ownership.**

   After a brief moment, the selected devices display a Configuration Status of **Deployed.**

3. **Repeat for remaining MPs and IPFEs**

   Repeat steps 1 and 2 for all remaining newly created MPs.
### 4.7 Configure Signaling Network Routes

**Procedure 26. Configure the Signaling Network Routes**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Establish GUI session on the NOAM VIP</td>
</tr>
</tbody>
</table>

This procedure configures signaling network routes on MP-type servers (DA-MP, IPFE, SBR, SS7-MP, etc.).

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.

![Oracle System Login](image-url)
Procedure 26. Configure the Signaling Network Routes

1. Navigate to **Main Menu->Configuration->Networking->Network->Routes**.
   - **Configuration**
   - **Networking**
   - **Networks**
   - **Routes**
   - **Services**

2. Select the first MP Server you see listed on the first row of tabs as shown, and click the **Entire Server Group** link. Initially, no routes should display.

3. **NOAM VIP**: Add route
   - Click **Insert** at the bottom of the screen to add additional routes.

4. **Primary NOAM VIP GUI**: Add default route for MPs going through signaling network gateway (Optional)
   - **To delete the existing default route**:
     1. Log into the PRIMARY NOAM VIP GUI.
     2. Navigate to **Configuration->Networking->Networks**.
     3. Select the specific SO tab.
     4. Select the XMI network and click **Unlock**. Click **OK**.
     5. Navigate to **Configuration->Networking->Routes**.
     6. Select the Specific MP XMI route and click **Delete**.
     7. Click **OK**.
     8. Repeat the above steps for all required MPs to delete the XMI routes.
     9. Navigate to **Configuration->Networking->Networks**.
    10. Select the respective SOAM tab.
    11. Select the XMI network and click **Lock**.
    12. Click **OK**.
   - If your MP servers no longer have a default route, then you can insert a default route here, which uses one of the signaling network gateways.

3. **NOAM VIP**: Navigate to routes configuration screen
Procedure 26. Configure the Signaling Network Routes

### Insert Route on DMP1

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Type  &quot;</td>
<td>Net</td>
<td>Select a route type. [Default = N/A, Options = Net,</td>
</tr>
<tr>
<td>&quot;</td>
<td>Default</td>
<td>Host]</td>
</tr>
<tr>
<td>Device</td>
<td>eth3</td>
<td>Select the network device name through which to</td>
</tr>
<tr>
<td>&quot;</td>
<td></td>
<td>[A value is required]</td>
</tr>
<tr>
<td>Destination</td>
<td></td>
<td>The destination network address. [Default = N/A, F</td>
</tr>
<tr>
<td>Netmask</td>
<td></td>
<td>A valid netmask for the network route destination</td>
</tr>
<tr>
<td>Gateway IP  &quot;</td>
<td></td>
<td>The IP address of the gateway for this route.</td>
</tr>
<tr>
<td>&quot;</td>
<td></td>
<td>[Default = N/A]</td>
</tr>
</tbody>
</table>

- **Route Type:** Default
- **Device:** Select the signaling device directly attached to the network where the XSI default gateway resides.
- **Gateway IP:** The XSI gateway you wish to use for default signaling network access.

13. Click **OK**.
Procedure 26. Configure the Signaling Network Routes

5. **Primary NOAM VIP GUI:** Add network routes for Diameter peers

1. Use this step to add IP4 and/or IPv6 routes to **Diameter** peer destination networks. The goal for this step is to ensure Diameter traffic uses the gateway(s) on the signaling networks.

   **Insert Route on BuenosAires-DAMP1**

   - **Route Type:** Net
   - **Device:** Select the appropriate signaling interface that is used to connect to that network
   - **Destination:** Type the Network ID of network to which the peer node is connected to
   - **Netmask:** Type the corresponding Netmask
   - **Gateway IP:** Type the IP of the customer gateway.

2. If you have more routes to enter, click **Apply** to save the current route entry. Repeat this step to enter more routes.

3. If you have finished entering routes, click **OK** to save the latest route and leave this screen.

6. **Repeat steps 2-5 for all other MP server groups**

The routes entered in this procedure should now be configured on all MPs in the server group for the first MP you selected. If you have additional MP server groups, repeat from step 2 but this time, select an MP from the next MP server group. Continue until you have covered all MP server groups.
### 4.8 Configure DSCP (Optional)

#### Procedure 27. Configure DSCP Values for Outgoing Traffic (Optional)

This procedure configures the DSCP values for outgoing packets on servers. DSCP values can be applied to an outbound interface as a whole, or to all outbound traffic using a specific TCP or SCTP source port. This step is optional and should only be executed if it has been decided that your network uses packet DSCP markings for Quality-of-Service purposes. Check off (√) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Primary NOAM VIP GUI: Establish GUI session on the NOAM VIP</td>
</tr>
</tbody>
</table>

Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.

![Oracle System Login](image)

Welcome to the Oracle System Login.

This application is designed to work with most modern HTML5 compliant browsers and uses both JavaScript and cookies. Please refer to the Oracle Software Web Browser Support Policy for details.

Unauthorized access is prohibited.

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

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.
Procedure 27. Configure DSCP Values for Outgoing Traffic (Optional)

**Primary NOAM VIP GUI:**
Option 1: Configure interface DSCP

**Note:** The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary.

1. Navigate to **Main Menu->Configuration->Networking->DSCP->Interface DSCP**.

2. Select the server to configure from the list of servers on the 2nd line. You can view all servers with **Entire Network** selected; or limit yourself to a particular server group by clicking on the server group name’s tab.

3. Click **Insert**.

4. Select the network **Interface** from the list, and type the **DSCP** value to apply to packets leaving this interface.

5. Click **OK** if there are no more interfaces on this server to configure, or **Apply** to finish this interface and continue with more interfaces by selecting them from the list and typing their **DSCP** values.
Procedure 27. Configure DSCP Values for Outgoing Traffic (Optional)

Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary.

1. Navigate to **Main Menu->Configuration->Networking->DSCP->Port DSCP**.

Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary.

2. Select the server to configure from the list of servers on the 2nd line. You can view all servers with **Entire Network** selected; or limit yourself to a particular server group by clicking on the server group name’s tab.

3. Click **Insert**.

4. Type the source **Port** and **DSCP** value, and select the transport **Protocol**.

5. Click **OK** if there are no more port DSCPs on this server to configure, or **Apply** to finish this port entry and continue entering more port DSCP mappings.

4. Repeat for additional servers

   Repeat steps 2-3 for all remaining servers.
4.9 Configure IP Front End (Optional)

Procedure 28. IP Front End (IPFE) Configuration

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>SOAM VIP: Login</strong> Log into the SOAM VIP GUI as the guiadmin user.</td>
</tr>
</tbody>
</table>

This procedure configures IP Front End (IPFE) and optimizes performance. Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number. If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
Procedure 28. IP Front End (IPFE) Configuration

2. **SOAM VIP:** Configuration of replication IPFE association data

1. Navigate to Main Menu->IPFE->Configuration->Options.

2. Type the IP address of the 1st IPFE in the IPFE-A1 IP Address field and the IP address of the 2nd IPFE in the IPFE-A2 IP Address field.

3. If applicable, type the address of the 3rd and 4th IPFE servers in IPFE-B1 IP Address and IPFE-B2 IP Address fields.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPFE-A1 IP Address</td>
<td>109.254.1.25 - IPFE1</td>
<td>IPv4 or IPv6 address of IPFE-A1. This selection is disabled when a Target Set has IPFE-A1 selected as Active.</td>
</tr>
<tr>
<td>IPFE-A2 IP Address</td>
<td>109.254.1.27 - IPFE2</td>
<td>IPv4 or IPv6 address of IPFE-A2. This selection is disabled when a Target Set has IPFE-A2 selected as Active.</td>
</tr>
<tr>
<td>IPFE-B1 IP Address</td>
<td>&lt;None&gt;</td>
<td>IPv4 or IPv6 address of IPFE-B1. This selection is disabled when a Target Set has IPFE-B1 selected as Active.</td>
</tr>
<tr>
<td>IPFE-B2 IP Address</td>
<td>&lt;None&gt;</td>
<td>IPv4 or IPv6 address of IPFE-B2. This selection is disabled when a Target Set has IPFE-B2 selected as Active.</td>
</tr>
</tbody>
</table>

**Note:** It is recommended the address reside on the IMI (Internal Management Interface) network.

**Note:** IPFE-A1 and IPFE-A2 must have connectivity between each other via these addresses. The same applies with IPFE-B1 and IPFE-B2.
Procedure 28. IP Front End (IPFE) Configuration

3. **SOAM VIP**: Configuration of IPFE target sets (Part 1)

1. Log into the **SOAM VIP** GUI as the **guiadmin** user.
2. Navigate to **Main Menu->IPFE->Configuration->Target Sets**.

   - **IPFE**
     - **Configuration**
     - **Options**
     - **Target Sets**

3. Click either **Insert IPv4** or **Insert IPv6** depending on the IP version of the target set you plan to use.

   This screen displays the following configurable settings:

   - **Protocols**: Protocols the target set supports.

     ![Protocols Table]

   - **Delete Age**: Specifies when the IPFE should remove its association data for a connection. Any packets presenting a source IP address/port combination that had been previously stored as association state but have been idle longer than the **Delete Age** configuration is treated as a new connection and does not automatically go to the same application server.

     ![Delete Age Configuration]

   - **Load Balance Algorithm**: Hash or Least Load options.

     ![Load Balance Algorithm Configuration]

   **Note**: For the IPFE to provide Least Load distribution, navigate to **Main Menu->IPFE->Configuration->Options**, Monitoring Protocol must be set to Heartbeat so the application servers can provide the load information the IPFE uses to select the least-loaded server for connections.

   ![IPFE Configuration]

   **Note**: The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios.

---

4. **SOAM VIP**: Configuration of IPFE target sets (Part 2)

1. Navigate to **Main Menu->IPFE->Configuration->Target Sets**.
Procedure 28. IP Front End (IPFE) Configuration

(Optional): If you have selected the Least Load algorithm, then you may configure the following fields to adjust the algorithm’s behavior:

**MPS Factor**: Messages per Second (MPS) is one component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). It is recommended that IPFE connections have Reserved Ingress MPS set to something other than the default, which is 0. To configure Reserved Ingress MPS, navigate to Main Menu ->Diameter->Configuration->Configuration Sets->Capacity Configuration. If you choose not to use Reserved Ingress MPS, set MPS Factor to 0, and Connection Count Factor, described below, to 100.

**Connection Count Factor**: This is the other component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very rapid rate) are a concern.

**Allowed Deviation**: Percentage within which two application server’s load calculation results are considered to be equal. If very short, intense connection bursts are expected to occur, increase the value to smooth out the distribution.

**Primary Public IP Address**: IP address for the target set.

*Note*: This address must reside on the XSI (External Signaling Interface) network because it is used by the application clients to reach the application servers. This address MUST NOT be a real interface address (that is, must not be associated with a network interface card).
Procedure 28. IP Front End (IPFE) Configuration

**Active IPFE:** IPFE to handle the traffic for the target set address.

**Secondary Public IP Address:** If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a Secondary IP Address.

---

### Note:
A secondary address is required to support SCTP multi-homing. A secondary address can support TCP, but the TCP connections are not multi-homed.

### Note:
If SCTP multi-homing is to be supported, select the mate IPFE of the Active IPFE for the Active IPFE for secondary address to ensure SCTP failover functions as designed.

**Target Set IP List:** Select an IP address, a secondary IP address if supporting **SCTP multi-homing**, a description, and a weight for the application server.

---

### Note:
The IP address must be on the XSI network since they must be on the same network as the target set address. This address must also match the IP version of the target set address (IPv4 or IPv6). If the Secondary Public IP Address is configured, it must reside on the same application server as the first IP address.

### Note:
If all application servers have an equal weight (for example, 100, which is the default), they have an equal chance of being selected. Application servers with larger weights have a greater chance of being selected.

2. Click **Add** to add more application servers (up to 16).
3. Click **Apply**.

---

### 5.
**SOAM VIP:** Repeat for additional configuration of IPFE target sets

- Repeat for steps 3 and 4 for each target set (up to 16).
- At least one target set must be configured.
### 4.10 SNMP Configuration (Optional)

**Procedure 29. Configure SNMP Trap Receiver(s) (Optional)**

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>NOAM VIP: Configure system-wide SNMP trap receiver(s)</td>
</tr>
</tbody>
</table>

1. Using a web browser, log into the NOAM VIP as the `guiadmin` user.

   Navigate to **Main Menu->Administration->SNMP**.

2. Click **Insert**.

3. Type the **IP address** or **Hostname** of the Network Management Station (NMS) to forward traps to. This IP should be reachable from the NOAM's XMI network.

4. Continue to add secondary manager IPs in the corresponding fields, if needed.

   Manager 1

   **Traps Enabled** checkboxes can be marked on a per manager basis.

   - Manager 1
   - Manager 2
   - Manager 3
   - Manager 4
   - Manager 5

5. Leave all other fields with their default values.

6. Click **OK**.
Procedure 29. Configure SNMP Trap Receiver(s) (Optional)

2. NOAM VIP: Enable traps from individual servers (Optional)

Note: By default, SNMP traps from MPs are aggregated and displayed at the active NOAM. If instead, you want every server to send its own traps directly to the NMS, then execute this procedure.

This procedure requires all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable.

1. Using a web browser, log into the NOAM VIP as the guiadmin user. Navigate to Main Menu->Administration->SNMP.

   - [Main Menu]
     - Administration
       - General Options
       - Access Control
       - Software Management
       - Remote Servers
         - LDAP Authentication
         - SNMP Trapping
         - Data Export
         - DNS Configuration

2. Make sure the Enabled checkbox is marked, if not, mark it as shown below:

   Traps from Individual Servers: Enabled

3. Click Apply and verify the data is committed.

4.11 Create iDIH Virtual Machines - VMware (Optional)

Procedure 30. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. N</td>
<td>Add the iDIH Oracle OVA to VMware</td>
</tr>
<tr>
<td>1. L</td>
<td>Launch the VMware client of your choice.</td>
</tr>
<tr>
<td>2. A</td>
<td>Add the iDIH Oracle OVA image to the VMware catalog or repository. Follow the instructions provided by the Cloud solutions manufacturer.</td>
</tr>
<tr>
<td>2. C</td>
<td>Create the Oracle VM from the OVA image</td>
</tr>
<tr>
<td>1. B</td>
<td>Browse the library or repository that you placed the iDIH Oracle OVA image.</td>
</tr>
<tr>
<td>2. D</td>
<td>Deploy the OVA image using vSphere Client or the vSphere Web Client.</td>
</tr>
<tr>
<td>3. N</td>
<td>Name the iDIH Oracle VM and select the data store.</td>
</tr>
</tbody>
</table>
### Procedure 30. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Configure resources for the iDIH Oracle VM</td>
</tr>
<tr>
<td>4.</td>
<td>iDIH Oracle VM Only: Create a raw storage block device (external device)</td>
</tr>
<tr>
<td>5.</td>
<td>Power on the iDIH Oracle VM</td>
</tr>
<tr>
<td>6.</td>
<td>iDIH Oracle VM Only: Verify the extra/second disk exists</td>
</tr>
<tr>
<td>7.</td>
<td>Repeat</td>
</tr>
</tbody>
</table>

**1.** Configure the **iDIH Oracle VM** per the resource profiles defined in [27] DSR Cloud Benchmarking Guide using the vSphere client or the vSphere web client.

**2.** Record the Ethernet addresses associated with each interface and the virtual network with which it is associated.

**Note:** Make sure the order of the interface creation is XMI, INT, and then IMI, if there is any. Only the Mediation VM requires the IMI interface.

**Note:** This step is **ONLY** required for iDIH Oracle VM.

Create an extra disk for the Oracle VM. Add the second disk using the vSphere client or the vSphere web client.

**3.**

**Note:** This step is **ONLY** required for iDIH Oracle VM.

Create an extra disk for the Oracle VM. Add the second disk using the vSphere client or the vSphere web client.

**4.**

**Note:** This step is **ONLY** required for iDIH Oracle VM.

Check if the raw storage block device (external disk) added in step 3 exits by executing any of these commands:

- `$ ls /dev/[sv]db`
- `$ fdisk -l`
- `$ df -h`

**Note:** Please DO NOT mount or format the added raw block device. Oracle ASM (Automatic Storage Management) automatically manages it. If you see it has been mounted, unmount it and make sure to completely remove the entry in the /etc/fstab.

**5.**

**Note:** This step is **ONLY** required for iDIH Oracle VM.

Repeat steps 1 through 6 for the following VMs. Use unique labels for the VM names:

- iDIH Application
- iDIH Mediation
### 4.12 Create iDIH Virtual Machines - KVM/OpenStack (Optional)

**Procedure 31. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)**

This procedure creates the iDIH Oracle, Mediation, and Application guest.

**Needed material:** iDIH Oracle OVA, iDIH Mediation OVA, and iDIH Application OVA

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Add the iDIH Oracle OVA to KVM/OpenStack</td>
</tr>
<tr>
<td>1.</td>
<td>Copy the OVA file to the OpenStack control node.</td>
</tr>
<tr>
<td>2.</td>
<td>Log into the OpenStack control node.</td>
</tr>
<tr>
<td>3.</td>
<td>In an empty directory, unpack the OVA file using <code>tar</code>.</td>
</tr>
<tr>
<td>4.</td>
<td>One of the unpacked files has a <code>.vmdk</code> suffix. This is the VM image file that must be imported.</td>
</tr>
<tr>
<td>5.</td>
<td>Source the OpenStack admin user credentials.</td>
</tr>
<tr>
<td>6.</td>
<td>Select an informative name for the new image.</td>
</tr>
<tr>
<td>7.</td>
<td>Import the image using the “glance” utility from the command line.</td>
</tr>
</tbody>
</table>

This process takes about 5 minutes depending on the underlying infrastructure.
### Procedure 31. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Create flavors for iDIH&lt;br&gt;Examine the storage recommendations in the resource profiles defined in [27] DSR Cloud Benchmarking Guide. A block storage must be created and attached for the Oracle VM. For example, create an idih.db for the Oracle database with an 100GB ephemeral disk.</td>
</tr>
<tr>
<td>3.</td>
<td>Create network interfaces&lt;br&gt;Examine the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide. Network ports must be created for each recommended interface. For example:</td>
</tr>
<tr>
<td>4.</td>
<td>Create and boot the iDIH VM instance from the glance image&lt;br&gt;1. Get the following configuration values. The image ID.&lt;br&gt;$ glance image-list&lt;br&gt;The flavor ID.&lt;br&gt;$ nova flavor-list&lt;br&gt;The network ID(s)&lt;br&gt;$ neutron net-list&lt;br&gt;An informative name for the instance. iDIH-Oracle&lt;br&gt;iDIH-Mediation&lt;br&gt;iDIH-Application</td>
</tr>
</tbody>
</table>
Procedure 31. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2.   | Create and boot the VM instance.  
The instance must be owned by the DSR tenant user, not the admin user. Source the credentials of the DSR tenant user and issue the following command. Use one --nic argument for each IP/interface. **Number of IP/interfaces for each VM type must conform with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.** **Note:** IPv6 addresses should use the v6-fixed-ip argument instead of v4-fixed-ip.  

**For Oracle VM Only**

Create the ephemeral storage for only the Oracle VM.

```
$ nova boot --image <image ID> --flavor <flavor id or name> --nic net-id=<xmi network id>,v4-fixed-ip=<xmi ip address> --nic net-id=<int network id>,v4-fixed-ip=<int ip address> --ephemeral size=100 --config-drive true <instance name>
```

For example:
```
$ nova boot --image 7e881048-190c-4b66-b26e-dc5b9dc3c07f --flavor idih.db --nic net-id=e96cb10a-9514-4702-b0c5-64fc99eb3fdd,v4-fixed-ip=10.250.65.161 --nic net-id=674b8461-ffed-4818-8dea-7544f9c06e5f,v4-fixed-ip=10.254.254.2 --ephemeral size=100 --config-drive true iDIH-Oracle
```

**For Application VM Only**

```
$ nova boot --image <image ID> --flavor <flavor id or name> --nic net-id=<xmi network id>,v4-fixed-ip=<xmi ip address> --nic net-id=<int network id>,v4-fixed-ip=<int ip address> --config-drive true <instance name>
```

For example:
```
$ nova boot --image 7e881048-190c-4b66-b26e-dc5b9dc3c07f --flavor idih.db --nic net-id=e96cb10a-9514-4702-b0c5-64fc99eb3fdd,v4-fixed-ip=10.250.65.161 --nic net-id=674b8461-ffed-4818-8dea-7544f9c06e5f,v4-fixed-ip=10.254.254.2 --config-drive true iDIH-Oracle
```

**For Mediation VM Only**

For Mediation, add the IMI interface as the IMI interface.

```
$ nova boot --image <image ID> --flavor <flavor id or name> --nic net-id=<xmi network id>,v4-fixed-ip=<xmi ip address> --nic net-id=<int network id>,v4-fixed-ip=<int ip address> --nic net-id=<imi network id>,v4-fixed-ip=<imi ip address> --config-drive true <instance name>
```

For example:
```
$ nova boot --image f548c2cd-1ddd-4c56-b619-b49a69af8801 --flavor idih --nic net-id=e96cb10a-9514-4702-b0c5-64fc99eb3fdd,v4-fixed-ip=10.250.65.162 --nic
```
**Procedure 31. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| **3.** | View the newly created instance using the nova tool.  
|     | `$ nova list --all-tenants`  
|     | The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool. |
| **5.** | Verify configured interface  
|     | If DHCP is enabled on the Neutron subnet, VM configures the VNIC with the IP address provided in step 4. To verify, ping the XMI IP address provided with the `nova boot`... command from step 4:  
|     | `$ ping <XMI-IP-Provided-During-Nova-Boot>`  
|     | If successfully pinging, ignore the step 6 to manually configuring the interface. |
| **6.** | Manually configure interface, if not already done (Optional)  
|     | **Note:** If the instance is already configured with an interface and has successfully pinged (step 5), then **ignore** this step to configure the interface manually.  
|     | 1. Log into the Horizon GUI as the DSR tenant user.  
|     | 2. Go to the Compute/Instances section.  
|     | 3. Click the **Name** field of the newly created instance.  
|     | 4. Select the **Console** tab.  
|     | 5. Login as the **admusr** user.  
|     | 6. Configure the network interfaces, conforming with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.  
|     | `$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask>`  
|     | `$ sudo netAdm add --onboot=yes --device=eth1 --address=<imi ip> --netmask=<imi net mask>`  
|     | `$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip>`  
|     | Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.  
|     | 7. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.  
|     | `$ sudo init 6`  
|     | The new VM should now be accessible via both network and Horizon consoles. |
| **7.** | Repeat  
|     | Repeat steps 1 through 4 for the following VMs. Use unique labels for the VM names:  
|     | iDIH-Application  
|     | iDIH-Mediation |
## 4.13 Create iDIH Virtual Machines - OVM-S/OVM-M (Optional)

**Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for each**

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
</table>
| This procedure imports the IDIH image and creates/configures a VM. Repeat this procedure three times for:  
- IDIH-Oracle (db)  
- IDIH-Application (app)  
- IDIH-Mediation (med) |

Replace XXX in variable names with the different suffix – when repeating.  

This procedure requires values for these variables:  
- `<OVM-M IP> = IP address to access a sh prompt on the OVM server`
- `<URL to IDIH-XXX OVA>= link(s) to a source for each IDIH product image (.ova)`
- `<MyRepository name> = name of the repository in the OVM to hold the product images (.ova)`
- `<ServerPool name>`
- `<VM name>`
- `<OVM network ID for XML>`
- `<OVM network ID for IDIH Internal>`
- `<OVM network ID for IMI>`

Execution of this procedure will discover and use the values of these variables:  
- `<Virtual Appliance IDIH-XXX OVA ID>`
- `<IDIH-XXX-OVA VM name_vm_vm>`
- `<VM id>`
- `<vCPUs Production>`
- `<Vnic 1 id>`
- `<size in GB>`
- `<VirtualDiskId>`
- `<VirtualDiskName>`
- `<Slot#>`

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.  

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
### Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for each

1. **Preparation:**
   - **Access command line of OVM**

   Refer to Common OVM Manager Tasks (CLI) for setting up the platform.

1. Get the site-specific values for these variables (overwrite example).
   - `<OVM-M IP> = 100.64.62.221`
2. Use the respective value for `<OVM-M IP>` into the command.
   - `ssh -l admin <OVM-M IP> -p 10000`
   - **Example:** `ssh -l admin 100.64.62.221 -p 10000`
   - Alternate: use a terminal emulation tool like putty.
### Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for each

<table>
<thead>
<tr>
<th></th>
<th>OVM-M CLI: Import the VirtualAppliance/OVA for IDIH-XXX</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td><strong>OVM-M CLI:</strong> Import the VirtualAppliance/OVA for IDIH-XXX</td>
</tr>
<tr>
<td></td>
<td>1. Use the respective values for <code>&lt;MyRepository name&gt;</code> and <code>&lt;URL to IDIH-XXX OVA&gt;</code> into the command.</td>
</tr>
<tr>
<td></td>
<td><strong>OVM&gt;importVirtualAppliance Repository name='MyRepository name' url=&quot;&lt;URL to IDIH-XXX OVA&gt;&quot;</strong></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>OVM&gt; importVirtualAppliance Repository name='XLab Utility Repo01' url=<a href="http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova">http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova</a></td>
</tr>
<tr>
<td></td>
<td>2. Execute the command and validate success.</td>
</tr>
<tr>
<td></td>
<td>3. Examine the screen results to find site-specific text for <strong>variables</strong> in these locations:</td>
</tr>
<tr>
<td></td>
<td><strong>Command:</strong> importVirtualAppliance Repository name='XLab Utility Repo01' url=<a href="http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova">http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova</a></td>
</tr>
<tr>
<td></td>
<td><strong>Status:</strong> Success</td>
</tr>
<tr>
<td></td>
<td><strong>Time:</strong> 2017-04-18 15:23:31,044 EDT</td>
</tr>
<tr>
<td></td>
<td><strong>JobId:</strong> 1492543363365</td>
</tr>
<tr>
<td></td>
<td><strong>Data:</strong></td>
</tr>
<tr>
<td></td>
<td>ID: 1128a1c6ce name: DSR-8.1.0.0.0_81.16.0.ova</td>
</tr>
<tr>
<td></td>
<td>4. Use the respective values for values for these variables (overwrite example).</td>
</tr>
<tr>
<td></td>
<td><code>&lt;Virtual Appliance IDIH-XXX OVA ID&gt; = 1128a1c6ce</code></td>
</tr>
</tbody>
</table>
Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for each

3. **OVM-M CLI**: Get the virtual appliance name. It is used in \(<\text{IDIH-XXX OVA VM name}>\) in later steps

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td><strong>OVM-M CLI</strong>: Get the virtual appliance name. It is used in (&lt;\text{IDIH-XXX OVA VM name}&gt;) in later steps</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Use the respective values for \(<\text{Virtual Appliance IDIH-XXX OVA ID}>\) in the command.

   \[\text{OVM}> \text{show VirtualAppliance id=<Virtual Appliance IDIH-XXX OVA id}>\]

   **Example:**

   \[\text{OVM}> \text{show VirtualAppliance id=1128a1c6ce}\]

2. Execute the command and validate success.

3. Examine the screen results to find site-specific text for variables in these locations:

   **Command:** \(\text{show VirtualAppliance id=1128a1c6ce}\)

   **Status:** Success

   **Time:** 2017-04-18 15:23:53,534 EDT

   **Data:**

   - \(\text{Origin} = \text{http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova}\)
   - \(\text{Repository} = 0004fb0000030000da5738315337bfc7 \ [XLab Utility Repo01]\)
   - \(\text{Virtual Appliance Vm 1} = 11145510c0\_vm\_vm\ [vm]\)
   - \(\text{Virtual Appliance VirtualDisk 1} = 11145510c0\_disk\_disk1\ [disk1]\)
   - \(\text{Id} = 11145510c0\ [\text{DSR-8.1.0.0.0_81.16.0.ova}]\)
   - \(\text{Name} = \text{DSR-8.1.0.0.0_81.16.0.ova}\)
   - \(\text{Description} = \text{Import URL: http://10.240.155.70/iso/DSR/8.1/ova/DSR-8.1.0.0.0_81.16.0.ova}\)
   - \(\text{Locked} = \text{false}\)

4. Use the respective values for these variables (overwrite example).

   \(<\text{IDIH-XXX-OVA VM name_vm_vm}> = 11145510c0\_vm\_vm\)
**Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for each**

<table>
<thead>
<tr>
<th></th>
<th>OVM-M CLI: Create a VM for IDIH-XXX OVA VM</th>
<th>Create a virtual machine from the virtual machine in the OVA virtual appliance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>OVM-M CLI: Create a VM for IDIH-XXX OVA VM</td>
<td>1. Use the respective value for <code>&lt;IDIH-db-OVA VM name_vm_vm&gt;</code> into the command.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>OVM&gt; createVmFromVirtualApplianceVm VirtualApplianceVm name=&lt;IDIH-XXX-OVA VM name_vm_vm&gt;</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>OVM&gt; createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Execute the command and validate success.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. Examine the screen results to find site-specific text for variables in these locations:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command: <code>createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Time: 2017-04-18 16:02:09,141 EDT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JobId: 1492545641976</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Data:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>id: 0004fb00000600004a0e02bdf9fc1bcd name: oracle-8.1.0.0.0_81.16.0.ova</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Use the respective values for these variables (overwrite example).</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>&lt;VM id&gt; = 0004fb00000600004a0e02bdf9fc1bcd</code></td>
</tr>
</tbody>
</table>

|   | OVM-M CLI: Add the VM to the server pool   | 1. Use the respective values for `<VM ID>` and `<ServerPool name>` into the command. |
|   |                                               | `OVM> add Vm id=<VM id> to ServerPool name="<ServerPool name>"` |
|   |                                               | Example: `OVM> add Vm id=0004fb00000600004a0e02bdf9fc1bcd to ServerPool name="XLab Pool 01"` |
|   |                                               | 2. Execute the command and validate success. |

*Note:* Refer Server Pool section in Appendix D.2 for further information on Server Pool.
Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for each

6. **OVM-M CLI**: Edit VM to apply required profile/resources


   ![Table](image)

<table>
<thead>
<tr>
<th>VM Name</th>
<th>vCPUs Lab</th>
<th>RAM (GB) Lab</th>
<th>vCPUs Production</th>
<th>RAM (GB) Production</th>
<th>Storage (GB) Lab and Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type of guest host</td>
<td>#</td>
<td>#</td>
<td>#</td>
<td>#</td>
<td>#</td>
</tr>
</tbody>
</table>

   2. Use the respective values for `<VM ID>`, `<VM name>`, and `<vCPUs Production>` into the command.

   **Example:**
   ```
   OVM> edit Vm id=<VM id> name=<VM name> memory=6144 memoryLimit=6144 cpuCountLimit=<vCPUs Production> cpuCount=<vCPUs Production> domainType=XEN_HVM description="<VM name>"  
   Example:  
   OVM> edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=na-noam-na-2a memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4 domainType=XEN_HVM description="na-noam-na-2a"  
   ```

   3. Execute the command and validate success.

   **Command:**
   ```
   edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=na-noam-na-2a memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4 domainType=XEN_HVM description="na-noam-na-2a"  
   Status: Success  
   Time: 2017-04-18 17:55:25,645 EDT  
   JobId: 1492552525477  
   ```

   Now, the VM has a name and resources.

   ![Table](image)

7. **OVM-M CLI**: Determine VNIC ID

   1. Use the respective value for `<VM name>` in the command.

   **Example:**
   ```
   OVM> show Vm name=<VM name>  
   Example:  
   OVM> show Vm name=na-noam-na-2a  
   ```

   2. Execute the command and validate success.

   3. Examine the screen results to find site-specific text for variables in these locations:

   ![Vnic 1](image)  
   ```
   <Vnic 1 ID> = 0004fb000007000091e1ab5ae291d8a  
   ```
## Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAAs and Create and Configure a VM for each

### 8. Determine network interfaces for the type of guest host

Refer to [27] DSR Cloud Benchmarking Guide to learn which network interfaces need to be configured for each guest type. The table looks like this:

<table>
<thead>
<tr>
<th>Type of guest host</th>
<th>OAM (XMI)</th>
<th>Local (IMI)</th>
<th>Sig A (XSI1)</th>
<th>Sig B (XSI2)</th>
<th>Sig C (XSI3-16)</th>
<th>Rep (SBR)</th>
<th>DIH Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
<td>eth#</td>
</tr>
</tbody>
</table>

**Note:** The VNICs need to be created in the correct order so the interfaces are associated with the correct network.

### 9. OVM-M CLI: Add (attach) XMI VNIC ID of the XMI network to VM (if required by guest host type)

1. Use the respective values for `<Vnic 1 ID>` and `<OVM network ID for XMI>` into the command

   ```bash
   OVM> add Vnic ID=<Vnic 1 ID> to Network name=<OVM network ID for XMI>
   ```

   Example:
   ```bash
   OVM> add Vnic ID=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9
   ```

2. Execute the command and validate success.

### 10. OVM-M CLI: Create and attach IDIH Internal VNIC to VM (if required by guest host type)

1. Use the respective values for `<OVM network ID for IDIH Internal>` and `<VM name>` into the command

   ```bash
   OVM> create Vnic network=<OVM network id for IDIH Internal> name=<VM name>-int on Vm name=<VM name>
   ```

   Example:
   ```bash
   OVM> create Vnic network=DIH Internal name=na_idih-db-int on Vm name=na_idih-db
   ```

2. Execute the command and validate success.

### 11. OVM-M CLI: Create and attach IMI VNIC ID to VM (if required by guest host type)

1. Use the respective values for `<OVM network ID for IMI>` and `<VM name>` into the command.

   ```bash
   OVM> create Vnic network=<OVM network ID for IMI> name=<VM name>-IMI on Vm name=<VM name>
   ```

   Example:
   ```bash
   OVM> create Vnic network=102e89a481 name=na-noam-na-2a-IMI on Vm name=na-noam-na-2a
   ```

2. Execute the command and validate success.
Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVA s and Create and Configure a VM for each

12. [IDIH Oracle VM Only] OVM-M

CLI: Create a raw storage block device (external device)

Create an extra virtual disk (only required on IDIH-Oracle (db) if the system is using OVM).

1. Decide on a name for the virtual disk: <VirtualDiskName>

2. Refer the resource profiles defined in [27] DSR Cloud Benchmarking Guide to learn the required GB of Storage for the IDIH type: <size in GB>

3. Use the respective value for <MyRepository Name> into the command.

   OVM> create VirtualDisk name='<VirtualDiskName>'
   size=<size in GB> sparse=<Yes/No> shareable=<Yes/No> on Repository name='<MyRepository Name>'

   Example:

   OVM> create VirtualDisk name=idih-db_disk1 size=100 sparse=No shareable=No on Repository name='XLab Utility Repo01'

4. Examine the screen results to find site-specific text for variables in these locations:

   Command: create VirtualDisk name=idih-db_disk size=100 sparse=No shareable=No on Repository name='XLab Utility Repo01'

   Status: Success
   Time: 2017-04-24 15:29:12,502 EDT
   JobId: 1493061481113
   Data:

   id:0004fb00001200001bae7adbe6b20e19.img  name:idih-db_disk

5. Use the respective values for these variables (overwrite example).

   <VirtualDiskId> = 0004fb00001200001bae7adbe6b20e19.img
   <VirtualDiskName> = idih-db_disk
Procedure 32. (OVM-S/OVM-M). Import Three IDIH OVAs and Create and Configure a VM for each

13. **[IDIH Oracle VM Only] OVM-M CLI:** Map the created virtual disk to a slot on the VM

   1. Decide on a slot for the virtual disk: `<Slot#>`
   2. Use the respective values for `<Slot#>` & `<VirtualDiskId>` & `<VirtualDiskName>` & `<VM name>` into the command.

      ```
      OVM> create VmDiskMapping slot=<Slot#> virtualDisk=<VirtualDiskId> name="<VirtualDiskName>" on Vm name=<VM name>
      ```

      Example:

      ```
      OVM> create VmDiskMapping slot=2 virtualDisk=0004fb00001200001bae7adbe6b20e19.img name='idih-db_disk' on Vm name=na_idih-db
      ```

   3. Execute the command and validate success.

      ```
      Command: create VmDiskMapping slot=2 virtualDisk=0004fb00001200001bae7adbe6b20e19.img name='idih-db_disk' on Vm name=na_idih-db
      ```

      Status: Success

      Time: 2017-04-24 15:32:50,875 EDT

      JobId: 1493062370724

      Data:

      ```
      id:0004fb00001300005ab9b00e6d47add name:idih-db_disk
      ```

14. **OVM-M CLI:** Start VM

   1. Use the respective value for `<VM name>` into the command

      ```
      OVM> start Vm name=<VM name>
      ```

      Example:

      ```
      OVM> start Vm name=na_idih-db
      ```

   2. Execute the command and validate success

15. **Repeat**

   Repeat steps 2 through 14 for the following VMs. Use Unique labels for the VM names:

   - iDIH-Application
   - iDIH-Mediation

4.14 Configure iDIH Virtual Machines (Optional)

Procedure 33. Configure iDIH VM Networks (Optional)

This procedure configures the iDIH guest VM external management networks.
Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. **Log into the Oracle VM console**
   1. Access the iDIH Oracle VM console.
   2. Login as the admusr user.
### Procedure 33. Configure iDIH VM Networks (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td><strong>(Oracle VM only)</strong> Verify the extra/second disk exists</td>
</tr>
</tbody>
</table>
|      | **Note:** This step is required **ONLY** for the Oracle VM. Check if the raw storage block device (external disk) exists by executing any of below commands (similar to the screenshot):
|      | $ ls /dev/[sv]db
|      | $ sudo fdisk -l
|      | $ df -h

**Note:** Please DO NOT mount or format the added raw block device. Oracle ASM (Automatic Storage Management) automatically manages it. To verify it, execute the following command:

$ df

If you see it has been mounted, unmount it and completely remove the entry in the `/etc/fstab`.

$ sudo netAdm delete --device=eth0

| 3.   | Delete the eth0 interface |

| 4.   | Trigger net rules file creation |
|      | Run the udevadm command to recreate net rules file. |
|      | $ sudo udevadm trigger --subsystem-match=net

**Note:** If this command does not create the net rules file, create it manually. Refer to Sample Net Rules File.
### Procedure 33. Configure iDIH VM Networks (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 5.   | Modify the ethernet interface names in the net rules file. Update the net rules file to replace the default interfaces names ethX with XMI and INT interfaces names. Replace eth0 with XMI; and eth1 with INT interface. Also, respective MAC addresses should be updated for each interface in lower case. MAC addresses can be determined using ifconfig -a command from the console.

*Note:* The Mediation VM requires the user to rename a third interface: eth2 as IMI interface.

2. Refer to Sample Net Rules File for a sample net rules file.  

   ```bash
   $ sudo vi /etc/udev/rules.d/70-persistent-net.rules
   ```

3. Reboot the VM.

   ```bash
   $ sudo init 6
   ```

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 6.   | As admusr on the Oracle VM configure the networks with netAdm.  

1. Log into the iDIH Oracle VM console as the admusr user.

2. The XMI network should already exist, but it can be created with the following command.

   ```bash
   $ sudo netAdm add --device=xmi --address=<IP Address in External Management Network> --netmask=<Netmask> --onboot=yes
   ```

3. Configure the int network IP address and netmask.

   ```bash
   $ sudo netAdm add --device=int --address=10.254.254.2 --netmask=255.255.255.224
   ```

   *Note:* Oracle VM internal IP = 10.254.254.2; the Mediation VM internal IP = 10.254.254.3; and the application internal IP address = 10.254.254.4. The netmasks for all is 255.255.255.224.

4. **Mediation Only.** If this is a Mediation VM, configure the Mediation internal management network.

   ```bash
   $ sudo netAdm add --device=imi --address=<IP Address in Internal Management Network> --netmask=<Netmask>
   ```

5. Configure the default gateway.

   ```bash
   $ sudo netAdm add --route=default --gateway=<gateway address for the External Management Network> --device=xmi
   ```

The VM network configuration has been completed. You should be able to ssh into the server through XMI interface.
Procedure 33. Configure iDIH VM Networks (Optional)

7. As admusr on the Oracle VM configure NTP and the Oracle VM hostname

   1. On the Oracle VM console, launch the platform configuration menu.
      
      $ sudo su - platcfg

   2. From the platform configuration menu configure ntpserver1 with the IP address supplied for NTP.
      
      Navigate to Network Configuration->NTP->Edit->ntpserver1.
      
      Click Yes when asked to restart NTP.

   3. Exit the network configuration menu.

   4. Configure the Oracle VM hostname.
      
      Navigate to Server Configuration->Hostname->Edit.
      
      **Note:** Typically, we select hostname and identify the host as iDIH application, iDIH Mediation, and iDIH Oracle.

   5. Exit the platform configuration menu.

8. Repeat

   Repeat Steps 1 through 7 for the following VMs. Use unique labels for the VM names:
   
   iDIH Mediation
   iDIH Application

4.15 Post iDIH Installation Configuration (Optional)

Procedure 34. Run Post Installation Scripts on iDIH VMs (Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log into the iDIH Oracle VM Console</td>
</tr>
<tr>
<td></td>
<td>1. Access the iDIH Oracle VM console.</td>
</tr>
<tr>
<td></td>
<td>2. Login as the admusr user.</td>
</tr>
<tr>
<td>2.</td>
<td>Run the iDIH Oracle post installation script</td>
</tr>
<tr>
<td></td>
<td>1. Wait for the software upgrades to complete on all iDIH VMs.</td>
</tr>
<tr>
<td></td>
<td>2. As admusr on the iDIH Oracle VM console, run the Oracle post installation script.</td>
</tr>
<tr>
<td></td>
<td>$ sudo /opt/xIH/oracle/configureOracle.sh</td>
</tr>
</tbody>
</table>

**Note:** The Oracle post installation script runs for 5 to 15 minutes depending on the Oracle version and patch level. Wait for it to complete before the next step is executed. Once the script execution is over, it will come out without any message.

**Note:** To verify the install status, check the /var/TKLC/xIH/log/oracle/post_image_install.log file for any errors. The error stating: "Cannot use backup/restore functions while using dispatcher" can safely be ignored.
### Procedure 34. Run Post Installation Scripts on iDIH VMs (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Log into the iDIH Mediation VM Console as admusr</td>
</tr>
<tr>
<td>4.</td>
<td>Run the iDIH Mediation VM post installation script</td>
</tr>
<tr>
<td>5.</td>
<td>Log into the iDIH application VM console as admusr</td>
</tr>
<tr>
<td>6.</td>
<td>Run the iDIH Application post installation script</td>
</tr>
</tbody>
</table>

#### 1. Access the iDIH Mediation VM console.

#### 2. Login as the admusr user.

#### 4. Run the iDIH Mediation VM post installation script

The Oracle post installation script must come to completion before the Mediation post installation script is run.

1. As the admusr user on the iDIH Mediation VM console, run the Mediation post installation script.

   ```bash
   $ sudo /opt/xIH/mediation/install.sh
   ```

**Note:** The Mediation post installation script runs for 2 to 10 minutes. Wait for it to complete before the next step is executed. To verify the install status, check the `/var/TKLC/xIH/log/mediation/post_image_install.log` file for any errors.

**Note:** It is assumed network configuration and functionality is correct before installation. If you encounter an issue of the mediation post installation script `/opt/xIH/mediation/install.sh` hanging at the beginning as shown below, but you are still able to ssh to 10.254.254.2, make sure the internal interface(int) MTU has the correct setting - 1500 MTU. If yes, MTU size adjustment may be needed. For verification, connect to oracle using sqlplus using the following commands:

   a. Log into the Mediation server as admusr.
   b. Execute the command `sudo su - tekelec`.
   c. Execute the command `sqlplus /@NSP`.

2. As tekelec on the iDIH Mediation VM console, run the following commands.

   ```bash
   $ sudo su - tekelec
   $ med:/usr/TKLC/xIH iset -fnodeName='hostname' -fhostName='hostname' NodeInfo where 1=1
   ```

#### 5. Log into the iDIH Application VM console as admusr

#### 6. Run the iDIH Application post installation script

The Mediation post installation script must come to completion before the Application post installation script is run.

As the admusr user on the iDIH Application VM console, run the Application post installation script.

```bash
$ sudo /opt/xIH/apps/install.sh
```

**Note:** The application post installation script runs for 2 to 10 minutes. Wait for it to complete before executing the next step.
Procedure 34. Run Post Installation Scripts on iDIH VMs (Optional)

Run the iDIH health check script on each of the iDIH VMs

7. Run the iDIH health check script on each of the iDIH VMs

Once all of the iDIH VMs have restarted. Run the health check scripts on each iDIH VM.

1. As the admusr user on the iDIH Oracle VM console, run the health check script and verify the results. Ignore the NTP message stating the tvoe-host is not integrated.

   $ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i

2. As admusr on the iDIH Application VM console, run the health check script and verify the results. Ignore the NTP message stating tvoe-host is not integrated.

   $ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i

3. As admusr on the iDIH Mediation VM console, run the health check script and verify results. Ignore the NTP message stating tvoe-host is not integrated.

   $ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh –i

Note: Ignore NTP message stating the tvoe-host is not integrated.

Procedure 35. Configure DSR Reference Data Synchronization for iDIH (Optional)

This procedure configures DSR reference data synchronization for iDIH.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

STEPS

1. iDIH Application Server: Login

   1. Establish an SSH session to the iDIH Application Server.
   2. Login as the admusr user.
   3. Issue the following command to login as a tekelec user.

      $ sudo su - tekelec

2. iDIH Application Server: Execute configuration script

   1. Execute the following script:

      Apps/trda-config.sh

      Example output:

      corsair-app:/usr/TKLC/xIH/apps/trda-config.sh
      dos2unix: converting file
      /usr/TKLC/xIH/bea/user_projects/domains/tekelec/nsp/trace-refdata-ad

      Please enter DSR oam server IP address: 10.240.39.175
      SQL*Plus: Release 12.1.0.2.0 Production on Thu Oct 1
      15:04:40 2015
      Connected to:
Procedure 35. Configure DSR Reference Data Synchronization for iDIH (Optional)

Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options

SQL> SQL> 2 3 4 5
1 row merged.
SQL>
Commit complete.

SQL> Disconnected from Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production
With the Partitioning, Automatic Storage Management, OLAP, Advanced Analytics and Real Application Testing options

Buildfile: /usr/TKLC/xIH/apps/trace-refdata-adapter/build.xml
app.disable:
common.weblogic.stop:
    [echo]
    [echo]
    [echo]
=================================
    [echo] application: xihtra
    [echo] date: 2015-10-01 15:04:41
    [echo]
=================================
    [echo] === stop application EAR
    [echo] date: 2015-10-01 15:04:41
    [java] weblogic.Deployer invoked with options: -adminurl t3://appserver:7001 -userconfigprojects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -stop
    [java] <Oct 1, 2015 3:05:08 PM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating
    [java] Task 24 initiated: [Deployer:149026]stop application xIH Trace Reference Data Adapter
    [java] Task 24 completed: [Deployer:149026]stop application xIH Trace Reference Data Adapter
    [java] Target state: stop completed on Server nsp
    [java]
BUILD SUCCESSFUL
Total time: 29 seconds
### Procedure 35. Configure DSR Reference Data Synchronization for iDIH (Optional)

| Buildfile: /usr/TKLC/xIH/apps/trace-refdata-adapter/build.xml | ![Code Snippet]
| --- | --- |
| app.enable: | ![Code Snippet]
| common.weblogic.start: | ![Code Snippet]
| [echo] | ![Code Snippet]
| [echo] | ![Code Snippet]
| [echo] | ![Code Snippet]
| ============================================================== | ![Code Snippet]
| [echo] application: xihtra | ![Code Snippet]
| [echo] date: 2015-10-01 15:05:10 | ![Code Snippet]
| [echo] | ![Code Snippet]
| ============================================================== | ![Code Snippet]
| [echo] === start application EAR | ![Code Snippet]
| [echo] date: 2015-10-01 15:05:10 | ![Code Snippet]
| [java] <Oct 1, 2015 3:05:56 PM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating | ![Code Snippet]
| [java] Target state: start completed on Server nsp | ![Code Snippet]
| [java] BUILD SUCCESSFUL | ![Code Snippet]
| Total time: 1 minute 17 seconds | ![Code Snippet]

2. When asked to "Please enter DSR OAM server IP address", type the VIP of the DSR SOAM (or active DSR SOAM if VIP is not available) and click Enter.

**Note:** If the address typed is unreachable, the script exits with error “Unable to connect to <ip-address>!”

1. Monitor the log file located at: `/var/TKLC/xIH/log/apps/weblogic/apps/application.log`
2. Examine the log file for entries containing text "Trace Reference Data Adapter".

<table>
<thead>
<tr>
<th>iDIH Application Server</th>
<th>Monitor completion</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Checkmark]</td>
<td>![Checkmark]</td>
</tr>
</tbody>
</table>
### Procedure 35. Configure DSR Reference Data Synchronization for iDIH (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td><strong>iDIH Application Server</strong> (Optional): Switch iDIH from one DSR to another DSR in a different network</td>
</tr>
</tbody>
</table>

**Note:** This is an optional step which is needed to switch an IDIH from one DSR to another DSR in a different network.

1. Establish an SSH session to the iDIH Application Server.
2. Login as the *tekelec* user
3. Execute these commands:
   a. `cd /usr/TKLC/xIH/apps/trace-refdata-adapter`
   b. `ant clean.data`
   c. `cd /usr/TKLC/xIH/apps/xihoam`
   d. `ant imp.init` (flush comagent connection data)
   e. `cd /usr/TKLC/xIH/apps/trace-refdata-adapter`
   f. `ant app.enable` (Sync MOs from SOAM)
   g. `cd /usr/TKLC/xIH/apps`
   h. `./trda-config.sh <DSR SOAM VIP in different network>`

### Procedure 36. iDIH Configuration: Configuring the SSO Domain (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>NOAM VIP GUI:</strong> Login</td>
</tr>
</tbody>
</table>

This procedure configures the SSO domain for iDIH.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. Establish a GUI session on the NOAM server by using the VIP IP address of the NOAM server. Open the web browser and type `https://<Primary_NOAM_VIP_IP_Address>` as the URL.
2. Login as the *admusr* user.
Procedure 36. iDIH Configuration: Configuring the SSO Domain (Optional)

2. NOAM VIP GUI: Configure DNS

1. Navigate to **Main Menu->Administration->Remote Servers->DNS Configuration**.

   - Remote Servers
     - LDAP Authentication
     - SNMP Trapping
     - Data Export
     - DNS Configuration

2. Select the NOAM tab.

   ![Main Menu: Administration -> Remote Servers -> DNS Configuration](image)

3. Configure values for the following fields:
   - Domain Name
   - Name Server
   - Search Domain 1

   ![External DNS Name Server](image)

4. If values have already been configured, click **Cancel**; otherwise configure the values and click **OK**.
Procedure 36. IDIH Configuration: Configuring the SSO Domain (Optional)

3. NOAM VIP GUI: Establish SSO local zone


2. Click Establish SSO Zone.

3. Type a value for Zone Name.

4. Click OK.

5. Click Report.

6. The Certificate Report displays. Select and copy the encoded certificate text to the clipboard for future access.

Example of Certificate Report:

-----BEGIN CERTIFICATE-----
MIICzkCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHEExCzAJBgNV
BAYTAlVTMQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWNhDEM0MDA1UEwGb3
TGJhY2xldGlzdCOVERa3NjNTRaMTkxMDQxNDIzNTRaMCcG
BgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBAQUAA4GkMEQwIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBAgIBA
### Procedure 36. iDIH Configuration: Configuring the SSO Domain (Optional)

<table>
<thead>
<tr>
<th>Step</th>
<th>iDIH Application Server GUI: Login</th>
<th>iDIH Application Server GUI: Launch the OAM portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.</td>
<td>Establish a GUI session on the iDIH application server. &lt;br&gt;https://&lt;app server IP&gt; &lt;br&gt;Login as the idihadmin user.</td>
<td>Navigate to the OAM portal icon to start the OAM web application.</td>
</tr>
<tr>
<td>5.</td>
<td><img src="https://example.com/idih.png" alt="iDIH Application Server GUI" /></td>
<td><img src="https://example.com/maintenance.png" alt="Maintenance" /></td>
</tr>
</tbody>
</table>
Procedure 36. iDIH Configuration: Configuring the SSO Domain (Optional)

6. iDIH Application Server GUI: Configure the SSO domain

1. Navigate to System->Single Sign On.

2. Click the Edit Value icon.

3. Type a value for the Domain Name.  
   **Note:** This should be the same domain name assigned in the DSR NOAM DNS Configuration (step 2).

4. Click the Save icon.

5. Click the Refresh icon to display data saved for the remote zone.
Procedure 36. iDIH Configuration: Configuring the SSO Domain (Optional)

7. **iDIH Application Server GUI:** Configure the SSO Remote Zone

1. Navigate to **System->Single Sign On.**

   ![Oracle IDIH Interface]

   Select the **SSO Zones** tab.

2. Click the **Add** icon.

3. Type a value for field **Remote Name.**

4. For field **X.509 Certificate,** paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.

5. Click the **Save** icon.

6. Click the **Refresh** icon to display the data saved for remote zone.
Procedure 37. Integrate iDIH into DSR (Optional)

This procedure configures the iDIH connections to DSR.
Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.
If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

1. Configure the iDIH ComAgent connection on the NOAM

1. **Navigate to** Main Menu->Communication Agent->Configuration->Remote Servers.

2. **Click** Insert.

3. **Add the iDIH Mediation server.**

4. **For the Remote Server IP Address** field, type the IMI IP address of the iDIH Mediation server.

5. **For the IP Address Preference** field, select the IP protocol preference (if IPv6 and IPv4 are configured).

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Server Name a</td>
<td></td>
</tr>
<tr>
<td>Remote Server IPv4 IP Address</td>
<td></td>
</tr>
<tr>
<td>Remote Server IPv6 IP Address</td>
<td></td>
</tr>
<tr>
<td>Remote Server Mode `</td>
<td>Select</td>
</tr>
<tr>
<td>IP Address Preference</td>
<td>Com/Agent Network Preference</td>
</tr>
</tbody>
</table>

6. **Set the Remote Server Mode to Server.**
### Procedure 37. Integrate iDIH into DSR (Optional)

1. Navigate to **Main Menu -> Diameter -> Troubleshooting with iDIH -> Configuration -> Options**.

   - Troubleshooting with iDIH
   - Configuration
     - Traces
     - Options
     - Global Options
     - Maintenance

2. Configure the Troubleshooting with iDIH on the SOAM

3. Type the fully qualified iDIH host name (or IP address) in the iDIH Visualization Address field:

   ![iDIH Configuration](image)

4. Click **Apply**.

### Procedure 38. iDIH Configuration: Configure the Mail Server (Optional)

**Note:** This procedure is optional; however, this option is required for security (password initialization set to AUTOMATIC) and forwarding (forwarding by mail filter defined), and is available only on the Application server.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>S T E P #</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1. iDIH Application Server: Login | 1. Establish an SSH session to the iDIH Application server.  
2. Login as the **admusr** user. |
Procedure 38. iDIH Configuration: Configure the Mail Server (Optional)

1. From the platcfg menu, type the following command:
   `sudo su - platcfg`

2. Select Application Server Configuration.

3. Select SMTP Configuration.

4. Select Edit.

5. Enter the following parameters:
   - Mail Server IP Address
   - User
   - Password
   - Email Address (From)
   - Mail smtp timeout
   - Mail smtp connectiontimeout
   - SNMP over SSL used?

6. Select OK.

7. Select Exit to exit the platcfg menu.
Procedure 39. iDIH Configuration: Configure SNMP Management Server (Optional)

| STEP | This procedure configures the SNMP management server.  
|      | **Note:** This procedure is optional; however, this option is required for forwarding (forwarding by SNMP filter defined), and is available only on the Application server.  
|      | Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.  
|      | If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.  

1. iDIH Application Server: Login  
   1. Establish an SSH session to the iDIH Application server.  
   2. Login as the admusr user.

2. iDIH Application Server: Configure the authenticated mail server  
   1. From the platcfg menu, type the following command:  
   
   ```
   $ sudo su - platcfg
   ```  
   2. Select **Application Server Configuration**.

3. Select **SNMP Agent Configuration**.

4. Select **Edit**.  
5. Enter the IP Address of the SNMP management server.  
   **Note:** The SNMP agent configuration is updated and the SNMP management server automatically restarts.  
6. Select **OK**.  
7. Select **Exit** to exit the platcfg menu.
### Procedure 40. iDIH Configuration: Change Network Interface (Optional)

This procedure changes the default network interface.

**Note:** Initially, the default network interface used to transport TTRs from DSR to DIH uses the internal IMI network; however, this can be changed, if required. It should be noted that changing this interface could degrade performance of TTR transmission.

**Note:** A script is provided to manage the settings so the operator does not need to know the details required to apply the settings. There are two settings `interface.name` and `interface.enabled`.

When `interface.enabled=True`, then communications over the `interface.name` value, where value is the name of the network interface as defined on the platform, is the only specified interface used for communications.

When `interface.enabled=False` then communications over the named interface is not enforced, that is, all interfaces configured on the platform are allowed to be used for communications.

For example, if it is required to use the XMI interface for communication instead of the default internal IMI interface, then the operator would supply `XMI` when asked for the interface name and `True` when asked if interface filtering should be applied.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>Step #</th>
<th>iDIH Mediation Server: Login</th>
<th>iDIH Mediation Server: Execute the change interface script</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Establish an SSH session to the iDIH Mediation server.</td>
<td>To execute the change interface script, type the following command:</td>
</tr>
<tr>
<td></td>
<td>1. Login as the <code>admusr</code> user.</td>
<td>$ chgIntf.sh</td>
</tr>
<tr>
<td></td>
<td>2. Type the following command to login as the <code>Tekelec</code> user.</td>
<td>2. Answer the questions during the script as follows.</td>
</tr>
<tr>
<td></td>
<td>$ sudo su - tekelec</td>
<td><strong>This script is used to change the interface name (default = imi) used for mediation communications and whether to enable network interface filtering or not. Please answer the following questions or enter CTRL-C to exit out of the script.</strong></td>
</tr>
</tbody>
</table>

Current setting are: `interface.name=imi`  
`interface.enabled=True`

Enter new network interface name, return to keep current [imi]: `xmi`  
Do you want to enable network interface filtering [True|False], return to keep current [True]:  
Updating configuration properties file with `interface.name=xmi` and `interface.enabled=True`, and restarting mediation configuration bundle...
4.16 Post-Install Activities

Procedure 41. Configure ComAgent Connections

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>SDS NOAM VIP GUI: Login</td>
</tr>
</tbody>
</table>

1. Establish a GUI session on the SDS NOAM server by using the VIP IP address of the NOAM server. Open the web browser and type https://<Primary_SDS_NOAM_VIP_IP_Address> as the URL.

2. Login as the admusr user.

Prerequisite: FABR application is activated.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
### Procedure 41. Configure ComAgent Connections

<table>
<thead>
<tr>
<th>Step</th>
<th>SDS NOAM VIP GUI: Configure remote server IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Navigate to <strong>Main Menu-&gt;Communication Agent-&gt;Configuration-&gt;Remote Servers.</strong></td>
</tr>
<tr>
<td></td>
<td>[Communication Agent] [Configuration] [Remote Servers] [Connection Groups] [Routed Services]</td>
</tr>
<tr>
<td>2.</td>
<td>Click <strong>Insert.</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>SDS NOAM VIP GUI: Configure remote server IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Type <strong>Remote Server Name</strong> for the DSR MP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Remote Server Name</strong>: ZombieDAMP1</td>
</tr>
<tr>
<td>2.</td>
<td>Type the <strong>Remote Server IMI IP address</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Remote Server IPv4 IP Address</strong>: 169.254.1.13</td>
</tr>
<tr>
<td></td>
<td><strong>Remote Server IPv6 IP Address</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This should be the IMI IP address of the DAMP server.</td>
</tr>
<tr>
<td>3.</td>
<td>Select <strong>Client</strong> for the Remote Server Mode from the list.</td>
</tr>
<tr>
<td></td>
<td><strong>Remote Server Mode</strong>: Client</td>
</tr>
<tr>
<td>4.</td>
<td>Select <strong>IP Address Preference</strong> (ComAgent Network Preference, IPv4, or IPv6) from the list.</td>
</tr>
<tr>
<td></td>
<td><strong>IP Address Preference</strong>: ComAgent Network Preference, IPv4 Preferred, IPv6 Preferred</td>
</tr>
<tr>
<td>5.</td>
<td>Select the <strong>Local Server Group</strong> from the available SDS DP server groups and click <strong>'Add'</strong> to assign.</td>
</tr>
</tbody>
</table>
Procedure 41. Configure ComAgent Connections

6. Click **Apply**.

4. **SDS NOAM VIP GUI**: Repeat

Repeat steps 2-3 for each remote MP in the same SOAM NE.
**Procedure 41. Configure ComAgent Connections**

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5.</strong> DSR NOAM VIP GUI: Login</td>
<td>1. Establish a GUI session on the DSR NOAM server by using the VIP IP address of the NOAM server. Open the web browser and type <strong>https://&lt;Primary_DSR_NOAM_VIP_IP_Address&gt;</strong> as the URL. 2. Login as the <strong>guiadmin</strong> user.</td>
<td></td>
</tr>
<tr>
<td><strong>6.</strong> DSR NOAM VIP GUI: Configure remote server IP address</td>
<td>1. Navigate to <strong>Main Menu-&gt;Communication Agent-&gt;Configuration-&gt;Remote Servers.</strong> 2. Click <strong>Insert.</strong></td>
<td></td>
</tr>
<tr>
<td><strong>7.</strong> DSR NOAM VIP GUI: Configure remote server IP address</td>
<td>1. Type <strong>Remote Server Name</strong> for the DSR MP server. 2. Type the <strong>Remote Server IMI IP address.</strong></td>
<td></td>
</tr>
</tbody>
</table>
Procedure 41. Configure ComAgent Connections

![ComAgent Connections](image)

**Note:** This should be the IMI IP address of the DP server.

3. Select **Server** for the Remote Server Mode from the list.

4. Select **IP Address Preference** (ComAgent Network Preference, IPv4, or IPv6) from the list.

5. Select the **Local Server Group** from the available DSR MP server groups and click ‘Add’ to assign.
### Procedure 41. Configure ComAgent Connections

6. Click **Apply**.

| 8. | DSR NOAM VIP GUI: Repeat | Repeat steps 6-7 for each remote DP in the same SOAM NE. |
| 9. | DSR NOAM VIP GUI: Configure connection groups | Navigate to **Main Menu->Communication Agent->Configuration->Connection Groups**. |
Procedure 41. Configure ComAgent Connections

10. **DSR NOAM VIP GUI: Edit connection groups**

1. Select the **DPSvcGroup** connection group.

<table>
<thead>
<tr>
<th>Connection Group</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPSvcGroup</td>
<td>0 Servers</td>
</tr>
</tbody>
</table>

2. Click **Edit**.

3. Select the **DP Servers** from the Available Servers in Network Element list and click **>>** to assign.

   **Editing existing Connection Groups**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Group Name</td>
<td>DPSvcGroup</td>
<td>Unique identifier used to label a Connection Group. [Default info. Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one must not start with a digit. [A value is required.]</td>
</tr>
</tbody>
</table>

   **Available Servers in Network Element**

<table>
<thead>
<tr>
<th>Available Servers in Network Element</th>
<th>Assigned Servers in Connection Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDSDP1</td>
<td></td>
</tr>
</tbody>
</table>

     **Editing existing Connection Groups**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Group Name</td>
<td>DPSvcGroup</td>
<td>Unique identifier used to label a Connection Group. [Default info. Range: A 32-character string. Valid characters are alphanumeric and underscore. Must contain at least one must not start with a digit. [A value is required.]</td>
</tr>
</tbody>
</table>

   **Available Servers in Network Element**

<table>
<thead>
<tr>
<th>Available Servers in Network Element</th>
<th>Assigned Servers in Connection Group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SDSDP1</td>
</tr>
</tbody>
</table>

4. Click **OK**.

11. **DSR NOAM VIP GUI: Verify servers in group**

Verify the correct number of servers are in the connection group.

<table>
<thead>
<tr>
<th>Connection Group</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>DPSvcGroup</td>
<td>1 Server</td>
</tr>
<tr>
<td></td>
<td>SDSDP1</td>
</tr>
</tbody>
</table>
### Procedure 42. Complete PCA Configuration (Optional)

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>This procedure completes PCA configuration.</td>
</tr>
<tr>
<td></td>
<td><strong>Prerequisite:</strong> PCA application is activated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td>1.</td>
<td>Complete PCA configuration</td>
<td>Refer to Section PCA Configuration of [2] DSR PCA Activation Guide for the steps required to complete PCA configuration.</td>
</tr>
</tbody>
</table>

### Procedure 43. Backups and Disaster Prevention

<table>
<thead>
<tr>
<th>STEP #</th>
<th>Task</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>This procedure provides instruction on backups and disaster prevention.</td>
</tr>
<tr>
<td></td>
<td><strong>Prerequisite:</strong> DSR and optional sub-systems are installed configured.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</td>
</tr>
<tr>
<td>1.</td>
<td>Backup from VIM</td>
<td>The preferred method of backing up cloud system VM instances is by snapshotting. Once the DSR and optional sub-systems are installed and configured, but before adding traffic, use the appropriate cloud tool such as the VMware Manager or the OpenStack Horizon GUI, to take snapshots of critical VM instances. It is particularly important to snapshot the control instances, such as the NOAM and SOAM.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> To be on the safer side, follow the below steps also to back up the NOAM and SOAM database</td>
</tr>
<tr>
<td>2.</td>
<td>Identify Backup Server</td>
<td>Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cloud Infrastructure Manager Server/Controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSR NOAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DSR SOAM</td>
</tr>
</tbody>
</table>
### Procedure 43. Backups and Disaster Prevention

<table>
<thead>
<tr>
<th></th>
<th>NOAM/SOAM VIP: Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td></td>
</tr>
</tbody>
</table>

1. Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server.

2. Open the web browser and enter a URL of:

   `http://<Primary_NOAM/SOAM_VIP_IP_Address>`

3. Login as the `guiadmin` user:

   ![Oracle System Login](image-url)
Procedure 43. Backups and Disaster Prevention

4. NOAM/SOAM VIP: Backup configuration data for the system

1. Navigate to Main Menu -> Status & Manage -> Database.
   - Status & Manage
     - Network Elements
     - Server
     - HA
     - Database
     - KPIs
     - Processes
     - Tasks
     - Files
   - Navigate to Main Menu -&gt; Status & Manage -&gt; Database.

2. Select the active NOAM server and click **Backup**.

3. Make sure the **Configuration** checkbox is marked.

4. Enter a filename for the backup and click **OK**.
Procedure 43. Backups and Disaster Prevention

5. **NOAM/SOAM VIP**: Verify the backup file existence.
   1. Navigate to **Main Menu -> Status & Manage -> Files**.
   2. Select the active NOAM or SOAM tab.
   3. The files on this server display. Verify the existence of the backup file.

6. **NOAM/SOAM VIP**: Download the file to a local machine.
   1. From the previous step, select the backup file.
   2. Click **Download**.
   3. Click **OK**.

7. **Upload the image to secure location**
   Transfer the backed up image to a secure location identified in step 2 where the server backup files are fetched in case of system disaster recovery.

8. **Backup active SOAM**
   Repeat **Steps 4 through 8** to back up the active SOAM.
### Procedure 44. (KVM/OpenStack Only) Configure Port Security

This procedure configures port security on TSA.

**Prerequisite:** Perform Enable the Neutron port security extension first. We require this extension to disable the Neutron anti-spoofing filter rules for a given port. Refer to Disable Port Security in Appendix F.6 where this is discussed.

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.

<table>
<thead>
<tr>
<th>STEP</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>IPFE with TSA only. Remove port security on TSA XMI network interfaces on IPFE and MP instances. If using IPFE with Target Set Addresses (TSA).</td>
</tr>
</tbody>
</table>

1.   Determine the TSA IP address as used in section 4.9, Procedure 28.
2.   Determine the corresponding XSI interface IP address as used in section 4.9, Procedure 28.
3.   Log into the OpenStack control node as the admusr user.
4.   Source the tenant user credentials.
5.   Determine security groups associated with the IPFE instance.

```
$ nova list-secgroup <VM instance ID>
```

**Note:** `<VM instance ID>` can be queried from the output of `nova list` command in the ID column for the given VM.

6.   Save the ID and names of the listed security groups for later use.
7.   Remove all listed security groups.

```
$ nova remove-secgroup <VM instance ID> <Security group ID>
```

**Note:** Use the `<VM instance ID>` and `<Security group ID>` as noted down in the step-6 above.

Alternatively, we can use the following syntax:

```
$ nova remove-secgroup <VM instance name> <Security group name>
```

8.   Determine the port ID of the XSI interface IP address from step 2 above.

```
$ neutron port-list -F id -F fixed_ips | grep <instance IP on TSA/XSI network>
```

**Note:** `<port ID>` is the value in first column of the output to this command.

9.   Disable port security for the port found in step 7.

```
$ neutron port-update <Port ID> --port-security-enabled=false
```

10. Re-enable port security for all the interfaces not on the TSA/XSI port used in step 9, including XMI, IMI, and others.

11. Determine the port IDs of the instance IP addresses not associated with the TSA/XSI network.

```
$ neutron port-list -F id -F fixed_ips | grep <instance IP not on TSA/XSI network>
```

12. For each of the non TSA/XSI instance ports perform the following
### Procedure 44. (KVM/OpenStack Only) Configure Port Security

Configure Port Security command for each of the security groups from step 6.

```
$ neutron port-update <Port ID> --security-group <Security group ID>
```

*Note:* Use the `<Security Group ID>` as noted down in the step-6 above.

### Procedure 45. Enable/Disable DTLS (SCTP Diameter Connections Only)

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Enable/Disable DTLS (SCTP Diameter connections only)</td>
</tr>
</tbody>
</table>

Oracle’s SCTP Datagram Transport Layer Security (DTLS) has SCTP AUTH extensions by default. SCTP AUTH extensions are required for SCTP DTLS. However, there are known impacts with SCTP AUTH extensions as covered by the CVEs referenced below. It is highly recommended that customers prepare clients before the DSR connections are established after installation. This ensures the DSR to client SCTP connection establishes with SCTP AUTH extensions enabled. See RFC 6083. If customers DO NOT prepare clients to accommodate the DTLS changes, then the SCTP connections to client devices WILL NOT establish after the DSR is installed.


Execute procedures in [22] DSR DTLS Feature Activation Procedure to disable/enable the DTLS feature.

### Procedure 46. Shared Secret Encryption Key Revocation (RADIUS Only)

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Revoke RADIUS shared secret encryption key</td>
</tr>
</tbody>
</table>

Refer to RADIUS Shared Secret Key revocation MOP to change the encryption key on the DSR installed setup. Refer to [23] DSR RADIUS Shared Secret Encryption Key Revocation MOP MO008572.

*Note:* It is highly recommended to change the key after installation due to security reasons.

### Procedure 47. DSR Performance Tuning

<table>
<thead>
<tr>
<th>Step #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This procedure changes tuning parameters for the system to achieve better performance.</td>
</tr>
</tbody>
</table>

Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.

If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.
Procedure 47. DSR Performance Tuning

1. Performance tuning (Optional)  
Refer Appendix H Performance Tuning Recommended for performance tuning on DSR.

Appendix A. Sample Network Element and Hardware Profiles

To enter all the network information for a network element into an AppWorks-based system, a specially formatted XML file needs to be filled out with the required network information. The network information is needed to configure both the NOAM and any SOAM network elements.

It is expected that the maintainer/creator of this file has networking knowledge of this product and the customer site at which it is being installed. The following is an example of a network element XML file.

The SOAM network element XML file needs to have same network names for the networks as the NOAM network element XML file has. It is easy to accidentally create different network names for NOAM and SOAM network elements, and then the mapping of services to networks are not possible.

```xml
<?xml version="1.0"?>
<networkelement>
  <name>NE</name>
  <networks>
    <network>
      <name>XMI</name>
      <vlanId>3</vlanId>
      <ip>10.2.0.0</ip>
      <mask>255.255.255.0</mask>
      <gateway>10.2.0.1</gateway>
      <isDefault>true</isDefault>
    </network>
    <network>
      <name>IMI</name>
      <vlanId>4</vlanId>
      <ip>10.3.0.0</ip>
      <mask>255.255.255.0</mask>
      <nonRoutable>true</nonRoutable>
    </network>
  </networks>
</networkelement>
```

Figure 3. Example Network Element XML File

Appendix B. List of Frequently Used Time Zones

This table lists several valid time zone strings that can be used for the time zone setting in a CSV file, or as the time zone parameter when manually setting a DSR time zone.
Table 5. List of Selected Time Zone Values

<table>
<thead>
<tr>
<th>Time Zone Value</th>
<th>Description</th>
<th>Universal Time Code (UTC) Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTC</td>
<td>Universal Time Coordinated</td>
<td>UTC-00</td>
</tr>
<tr>
<td>America/New_York</td>
<td>Eastern Time</td>
<td>UTC-05</td>
</tr>
<tr>
<td>America/Chicago</td>
<td>Central Time</td>
<td>UTC-06</td>
</tr>
<tr>
<td>America/Denver</td>
<td>Mountain Time</td>
<td>UTC-07</td>
</tr>
<tr>
<td>America/Phoenix</td>
<td>Mountain Standard Time — Arizona</td>
<td>UTC-07</td>
</tr>
<tr>
<td>America/Los Angeles</td>
<td>Pacific Time</td>
<td>UTC-08</td>
</tr>
<tr>
<td>America/Anchorage</td>
<td>Alaska Time</td>
<td>UTC-09</td>
</tr>
<tr>
<td>Pacific/Honolulu</td>
<td>Hawaii</td>
<td>UTC-10</td>
</tr>
<tr>
<td>Africa/Johannesburg</td>
<td></td>
<td>UTC+02</td>
</tr>
<tr>
<td>America/Mexico City</td>
<td>Central Time — most locations</td>
<td>UTC-06</td>
</tr>
<tr>
<td>Africa/Monrovia</td>
<td></td>
<td>UTC+00</td>
</tr>
<tr>
<td>Asia/Tokyo</td>
<td></td>
<td>UTC+09</td>
</tr>
<tr>
<td>America/Jamaica</td>
<td></td>
<td>UTC-05</td>
</tr>
<tr>
<td>Europe/Rome</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Asia/Hong Kong</td>
<td></td>
<td>UTC+08</td>
</tr>
<tr>
<td>Pacific/Guam</td>
<td></td>
<td>UTC+10</td>
</tr>
<tr>
<td>Europe/Athens</td>
<td></td>
<td>UTC+02</td>
</tr>
<tr>
<td>Europe/London</td>
<td></td>
<td>UTC+00</td>
</tr>
<tr>
<td>Europe/Paris</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Madrid</td>
<td>mainland</td>
<td>UTC+01</td>
</tr>
<tr>
<td>Africa/Cairo</td>
<td></td>
<td>UTC+02</td>
</tr>
<tr>
<td>Europe/Copenhagen</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Berlin</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Prague</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>America/Vancouver</td>
<td>Pacific Time — west British Columbia</td>
<td>UTC-08</td>
</tr>
<tr>
<td>America/Edmonton</td>
<td>Mountain Time — Alberta, east British Columbia &amp; west Saskatchewan</td>
<td>UTC-07</td>
</tr>
<tr>
<td>America/Toronto</td>
<td>Eastern Time — Ontario — most locations</td>
<td>UTC-05</td>
</tr>
<tr>
<td>America/Montreal</td>
<td>Eastern Time — Quebec — most locations</td>
<td>UTC-05</td>
</tr>
<tr>
<td>America/Sao Paulo</td>
<td>South &amp; Southeast Brazil</td>
<td>UTC-03</td>
</tr>
<tr>
<td>Europe/Brussels</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Australia/Perth</td>
<td>Western Australia — most locations</td>
<td>UTC+08</td>
</tr>
<tr>
<td>Australia/Sydney</td>
<td>New South Wales — most locations</td>
<td>UTC+10</td>
</tr>
<tr>
<td>Time Zone Value</td>
<td>Description</td>
<td>Universal Time Code (UTC) Offset</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Asia/Seoul</td>
<td></td>
<td>UTC+09</td>
</tr>
<tr>
<td>Africa/Lagos</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>Europe/Warsaw</td>
<td></td>
<td>UTC+01</td>
</tr>
<tr>
<td>America/Puerto Rico</td>
<td></td>
<td>UTC-04</td>
</tr>
<tr>
<td>Europe/Moscow</td>
<td>Moscow+00 — west Russia</td>
<td>UTC+04</td>
</tr>
<tr>
<td>Asia/Manila</td>
<td></td>
<td>UTC+08</td>
</tr>
<tr>
<td>Atlantic/Reykjavik</td>
<td></td>
<td>UTC+00</td>
</tr>
<tr>
<td>Asia/Jerusalem</td>
<td></td>
<td>UTC+02</td>
</tr>
</tbody>
</table>
### Appendix C. Common KVM/OpenStack Tasks

#### Appendix C.1 Create a Network Port

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create the network ports for the NO network interfaces.</td>
</tr>
</tbody>
</table>
| 2.   | Determine the IP address for the interface.  
    For eth0, the IP might be 10.x.x.157.  
    For eth1, the IP might be 192.168.x.157. |
| 3.   | Identify the neutron network ID associated with each IP/interface using the `neutron` command line tool.  
    Copy here: `$ neutron net-list` |
| 4.   | Identify the neutron subnet ID associated with each IP/interface using the `neutron` command line tool.  
    Copy here: `$ neutron subnet-list` |
| 5.   | Create the network port using the `neutron` command line tool, being sure to choose an informative name. Note the use of the subnet ID and the network ID (final argument).  
    Port names are usually a combination of instance name and network name.  
    NO1-xmi  
    SO2-imi  
    MP5-xsi2  
    The ports must be owned by the DSR tenant user, not the admin user. Either source the credentials of the DSR tenant user or use the DSR tenant user ID as the value for the `--tenant-id` argument.  
    Copy here: `$. keystonerc_dsr_user`  
    Copy here: `$. keystone user-list`  
    Copy here: `$ neutron port-create --name=NO1-xmi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=10.x.x.157 <network id>`  
    Copy here: `$ neutron port-create --name=NO1-imi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=192.168.x.157 <network id>`  
    View your newly created ports using the neutron tool.  
    Copy here: `$. neutron port-list` |
## Appendix C.2 Create and Boot OpenStack Instance

<table>
<thead>
<tr>
<th></th>
<th>Create a VM instance from a glance image</th>
<th>1. Get the following configuration values.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>The image ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ glance image-list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The flavor ID.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ nova flavor-list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The network ID(s)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$ neutron net-list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An informative name for the instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NO1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SO2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MP5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Create and boot the VM instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The instance must be owned by the DSR tenant user, not the admin user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Source the credentials of the DSR tenant user and issue the following command. Number of IP/interfaces for each VM type must conform with the OODSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The VM takes approximately 5 minutes to boot. At this point, the VM has no configured network interfaces and can only be accessed by the Horizon console tool.</td>
</tr>
</tbody>
</table>

### Note:
IPv6 addresses should use the `v6-fixed-ip` argument instead of `v4-fixed-ip`. 

```bash
$ nova boot --image <image ID> --flavor <flavor id> --nic net-id=<first network id>,v4-fixed-ip=<first ip address> --nic net-id=<second network id>,v4-fixed-ip=<second ip address> InstanceName
```

View the newly created instance using the nova tool.

```bash
$ nova list --all-tenants
```

The VM takes approximately 5 minutes to boot. At this point, the VM has no configured network interfaces and can only be accessed by the Horizon console tool.
# Appendix C.3 Configure Networking for OpenStack Instance

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Verify/Configure the network interface</td>
</tr>
<tr>
<td>2.</td>
<td>Check if the interface is configured automatically.</td>
</tr>
<tr>
<td>3.</td>
<td>If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address. To verify, ping the XMI IP address provided with the <code>nova boot</code> command:</td>
</tr>
<tr>
<td></td>
<td><code>$ping &lt;XMI-IP-Provided-During-Nova-Boot&gt;</code></td>
</tr>
<tr>
<td></td>
<td>If the ping is successful, ignore the next part to configure the interface manually.</td>
</tr>
<tr>
<td>4.</td>
<td>Manually configure the interface, if not already done (optional).</td>
</tr>
<tr>
<td></td>
<td>a. Log into the Horizon GUI as the DSR tenant user.</td>
</tr>
<tr>
<td></td>
<td>b. Go to the Compute/Instances section.</td>
</tr>
<tr>
<td></td>
<td>c. Click on the Name field of the newly created instance.</td>
</tr>
<tr>
<td></td>
<td>d. Select the Console tab.</td>
</tr>
<tr>
<td></td>
<td>e. Login as the admusr user.</td>
</tr>
<tr>
<td>5.</td>
<td>f. Configure the network interfaces, conforming with the OCDSR Network to Device Assignments defined in [27] DSR Cloud Benchmarking Guide.</td>
</tr>
<tr>
<td></td>
<td><code>$sudo netAdm add --onboot=yes --device=eth0 --address=&lt;xmi ip&gt; --netmask=&lt;xmi net mask&gt;</code></td>
</tr>
<tr>
<td></td>
<td><code>$sudo netAdm add --route=default --device=eth0 --gateway=&lt;xmi gateway ip&gt;</code></td>
</tr>
<tr>
<td>6.</td>
<td>Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.</td>
</tr>
<tr>
<td>7.</td>
<td>3. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.</td>
</tr>
<tr>
<td></td>
<td><code>$sudo init 6</code></td>
</tr>
<tr>
<td></td>
<td>The new VM should now be accessible via both network and Horizon console.</td>
</tr>
</tbody>
</table>

## Appendix D. Common OVM Manager Tasks (CLI)

### Appendix D.1 Setting Up the Server

**Note:** This section sets up the server using the command line interface of OVM Manager. All configurations/setup **can also be done** from the GUI/dashboard of OVM Manager.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Log into the OVM-M command line interface</td>
</tr>
<tr>
<td></td>
<td><code>ssh -l admin &lt;OVM-M IP&gt; -p 1000</code></td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td><code>[root@manager01 ~]# ssh -l admin 10.240.16.138 -p 10000 admin@10.240.16.138's password:</code></td>
</tr>
</tbody>
</table>
2. **OVM-M CLI:** Discover Oracle VM server
   
   Discover Oracle VM server
   
   `discoverServer ipAddress=value` `password=value` `takeOwnership= { Yes | No }`
   
   **Example:**
   
   OVM> `discoverServer ipAddress=10.240.16.139` `password=password` `takeOwnership=Yes`

3. **OVM-M CLI:** Create an ethernet-based network with the VM role
   
   Create an ethernet-based network with the VM role
   
   `create Network [ roles= { MANAGEMENT | LIVE_MIGRATE | CLUSTER_HEARTBEAT | VIRTUAL_MACHINE | STORAGE } ]` 
   `name=value [ description=value ] [ on Server instance ]`
   
   **Example:**
   
   OVM>`create Network name=XMI roles=VIRTUAL_MACHINE`

4. **OVM-M CLI:** Add a port from each Oracle VM server to the network
   
   **Note:** Skip this step and proceed to step 5 for bonded interfaces.
   
   1. Find the ID of an Ethernet port.
      
      OVM> `show Server name=MyServer1`
      
      ... 
      
      Ethernet Port 1 = 0004fb00002000007711332ff75857ee 
      [eth0 on MyServer3.virtlab.info]
      Ethernet Port 2 = 0004fb0000200000d2e7d2d352a6654e 
      [eth1 on MyServer3.virtlab.info]
      Ethernet Port 3 = 0004fb0000200000c12192a08f2236e4 
      [eth2 on MyServer3.virtlab.info]

   2. Add a port from each Oracle VM Server to the network.
      
      OVM>`add Port instance to { BondPort | Network } instance`
      
      **Example:**
      
      OVM>`add Port id=0004fb0000200000d2e7d2d352a6654e to Network name=MyVMNetwork`
5. **OVM-M CLI**: Create Bondport (For Bonded Interfaces)

1. Find the ID of an Ethernet port.
   
   ```
   OVM> list Port
   Status: Success
   Time: 2016-08-22 04:43:02,565 EDT
   Data:
   id:0004fb000020000045b4e8dc0b3acc6 name:usb0 on vms01.test.com
   id:0004fb00002000005fde208ce6392c0a name:eth4 on vms01.test.com
   id:0004fb0000200000b1dceeb39006d839 name:eth5 on vms01.test.com
   id:0004fb000020000027e3a02bc28dd153 name:eth2 on vms01.test.com
   id:0004fb0000200000fce443e0d30cd3d5 name:eth3 on vms01.test.com
   id:0004fb0000200000a908e402fc542312 name:eth0 on vms01.test.com
   id:0004fb0000200000247b03c2a4a90ec name:eth1 on vms01.test.com
   ```

2. Create Bondport on required interfaces.

   ```
   OVM> create BondPort
   ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server name=compute01.test.com
   Command: create BondPort
   ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server name=compute01.test.com
   Status: Success
   ```

6. **OVM-M CLI**: Add VLAN Interface to network (for VLAN tagged networks)

1. Find the ID of an Ethernet port.

   ```
   OVM> list BondPort
   Command: list BondPort
   Status: Success
   Time: 2016-08-22 04:38:22,327 EDT
   Data:
   id:0004fb00002000005a45a0761813d512 name:bond1
   id:0004fb0000200000645cfc865736cea8 name:bond0 on compute01.test.com
   ```

2. Create VLAN interface.

   ```
   OVM> create VlanInterface vlanId=43 name=bond1.43 on BondPort id=0004fb00002000005a45a0761813d512
   Command: create VlanInterface vlanId=43 name=bond1.43
3. **Add remaining VLAN interfaces to the same bond accordingly, like:**

   ```
   OVM> create VlanInterface vlanId=44 name=bond1.44 on BondPort id=0004fb000000005a45a0761813d512
   OVM> create VlanInterface vlanId=30 name=bond1.30 on BondPort id=0004fb000000005a45a0761813d512
   OVM> create VlanInterface vlanId=31 name=bond1.31 on BondPort id=0004fb000000005a45a0761813d512
   ```

4. **Add VLAN interfaces to network.**

   ```
   OVM> add VlanInterface name=bond1.43 to Network name=XMI
   Command: add VlanInterface name=bond1.43 to Network name=XMI
   Status: Success
   Time: 2016-08-22 05:14:29,321 EDT
   JobId: 1471857258238
   OVM> add VlanInterface name=bond1.44 to Network name=IMI
   Command: add VlanInterface name=bond1.44 to Network name=IMI
   Status: Success
   Time: 2016-08-22 05:15:24,216 EDT
   JobId: 1471857321329
   OVM> add VlanInterface name=bond1.30 to Network name=XSI1
   Command: add VlanInterface name=bond1.30 to Network name=XSI1
   Status: Success
   Time: 2016-08-22 05:15:39,190 EDT
   JobId: 1471857337005
   OVM> add VlanInterface name=bond1.31 to Network name=XSI2
   Command: add VlanInterface name=bond1.31 to Network name=XSI2
   Status: Success
   Time: 2016-08-22 05:15:52,576 EDT
   JobId: 1471857349684
   ```

7. □ **OVM-M CLI:** Create unclustered server pool

   **Note:** To create clustered server pool, ignore this step and proceed to next.

   ```
   OVM> create ServerPool clusterEnable=No name=MyServerPool description='Unclustered server pool'
   ```

8. **OVM-M CLI:**

   **Note:** Skip this step if an unclustered server pool is already created. This
Create clustered server pool (Optional)

1. To create a clustered server pool you must provide a file system or physical disk to use for the server pool file system. To find a file system or physical disk, use the list command:

   OVM> list FileSystem

   id:66a61958-e61a-44fe-b0e0-9dd64abef7e3 name:nfs on 10.172.76.125:/mnt/vol1/poolfs03
   id:0004fb0000050000b85745f78b0c4b61 name:fs on 350014ee2568cc0cf
   id:4e6bb1575-e61a-4662-87b9-a84b40ce3db7 name:nfs on 10.172.76.125:/mnt/vol1/poolfs04
   id:858d98c5-3d8b-460e-9160-3415cbda738 name:nfs on 10.172.76.125:/mnt/vol1/poolfs01
   id:0dea4818-20e6-4d3a-958b-b12cf91588b5 name:nfs on 10.172.76.125:/mnt/vol1/poolfs02
   id:35b4f1c6-182b-4ea5-9746-51393f3b515c name:nfs on 10.172.76.125:/mnt/vol2/repo03
   id:aeb6143d-0a96-4845-9690-740bfbfe225e name:nfs on 10.172.76.125:/mnt/vol1/repo01
   id:05e8536f-8d9c-4d7c-bbb2-29b3ffafe011 name:nfs on 10.172.76.125:/mnt/vol2/repo02
   id:0004fb00000500006a46a8dbd2461939 name:MyServerPool_cluster_heartbeat
   id:0004fb0000050000809e28f4fab56b1 name:fs on 350014ee20137ee44

   OVM> list PhysicalDisk

   id:0004fb000018000019b86ccf3f473a9e name:FreeBSD (9)
   id:0004fb00001800004609a67d55b5803 name:FreeBSD (3)
   id:0004fb0000180002179de6afe5f0cf3 name:SATA_WDC_WD5001ABYS_WD-WCAS86288968
   id:0004fb00001800020b43f9684fc78ac name:FreeBSD (2)
   id:0004fb0000180000732be086af26911 name:FreeBSD (7)
   id:0004fb00001800067ce80973e18374e name:FreeBSD (8)
   id:0004fb00001800035ce16ee4d58dc4d name:FreeBSD (1)
   id:0004fb0000180006855117242d9a537 name:FreeBSD (6)
   id:0004fb00001800009c7a87ba52ce5eb name:FreeBSD (5)
   id:0004fb000018000ebabef98381987d8 name:SATA_WDC_WD5001ABYS_WD-WCAS86571931
   id:0004fb00001800008f6ea92426f2c9b8 name:SATA_WDC_WD5001ABYS_WD-WCAS86257005
   id:0004fb00001800008cbb1925cbb2f81 name:SATA_WDC_WD5001ABYS_WD-WCAS86578538
2. Before you create a clustered server pool you must refresh the file system or physical disk to be used for the server pool file system. To refresh a file system:

   OVM> refresh { AccessGroup | Assembly | FileServer | FileSystem | PhysicalDisk | Repository | Server | StorageArray | VirtualAppliance } instance

   For example, to refresh a physical disk:

   OVM> refresh PhysicalDisk
   id=0004fb000018000035ce16ee4d58dc4d

3. Refresh a file system:

   OVM> refresh FileSystem name="nfs on 10.172.76.125://mnt//vol1//repo01"
   OVM> create ServerPool clusterEnable=Yes filesystem="nfs on 10.172.76.125://mnt//vol1//poolfs01" name=MyServerPool description='Clustered server pool'

9. OVM-M CLI: Add Oracle VM servers to the server pool

   OVM> add Server name=MyServer to ServerPool name=MyServerPool

10. OVM-M CLI: Create storage repository

    1. Find the physical disk (LUN) to use for creating the storage repository.

       OVM> list FileServer
       Command: list FileServer
       Status: Success
       Time: 2016-08-19 02:11:39,779 EDT
       Data:

       id:0004fb0000090000445dac29e88bc38 name:Local FS vms03.test.com
       id:0004fb000009000045715cad6f165ecf name:Local FS vms01.test.com
       id:0004fb0000090000df4cd9c3170092e4 name:Local FS vms02.test.com
       id:0004fb00000900064b96ed88a9a0185 name:Local FS vms04.test.com

    2. Find a local file system on an Oracle VM server that has access to the LUN.

       OVM> list FileServer
       Command: list FileServer
       Status: Success
       Time: 2016-08-19 02:11:39,779 EDT
       Data:

       id:0004fb0000090000445dac29e88bc38 name:Local FS vms03.test.com
id:0004fb000009000045715cad6f165ecf name:Local FS vms01.test.com
id:0004fb0000090000df4cd9c3170092e4 name:Local FS vms02.test.com
id:0004fb000009000064b96ed88a9a0185 name:Local FS vms04.test.com

3. Create file system.

OVM> create FileSystem name=VmsFs01
physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e490ac3f392" on FileServer name="Local FS vms01.test.com"
Command: create FileSystem name=VmsFs01
physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e490ac3f392" on FileServer name="Local FS vms01.test.com"
Status: Success
Time: 2016-08-19 02:22:46,581 EDT
JobId: 1471587738752
Data:
id:0004fb00000500006779d42da60c0be6 name:VmsFs01

4. Create repository.

OVM> create Repository name=Vms01Repo on FileSystem name=VmsFs01
Command: create Repository name=Vms01Repo on FileSystem name=VmsFs01
Status: Success
Time: 2016-08-19 02:24:04,092 EDT
JobId: 1471587843432
Data:
id:0004fb00000300003c8f771791114d53 name:Vms01Repo

5. Add server pool to repository.

OVM> add ServerPool name=TestPool001 to Repository name=Vms01Repo
Refresh the storage repository using the syntax:
OVM> refresh Repository name=MyRepository

Appendix D.2 Server Pool

A server pool is a required entity in Oracle VM, even if it contains a single Oracle VM Server. In practice, several Oracle VM servers form a server pool, and an Oracle VM environment may contain one or several server pools. Server pools are typically clustered, although an unclustered server pool is also possible. Server pools have shared access to storage repositories and exchange and store vital cluster information in the server pool file system. Refer [25] Oracle VM Concepts Guide for more information.
Appendix E. Firewall Ports

<table>
<thead>
<tr>
<th>Flow Description</th>
<th>Purpose</th>
<th>Protocol/Port</th>
<th>IP Protocol Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP flow for time sync</td>
<td>XMI network</td>
<td>UDP:123</td>
<td>IPv4, IPv6</td>
</tr>
<tr>
<td>hostname resolution (dns)</td>
<td>XMI, IMI Network</td>
<td>UDP/TCP: 53</td>
<td>IPv4, IPv6</td>
</tr>
<tr>
<td>SSH</td>
<td>XMI Network</td>
<td>TCP: 22</td>
<td>IPv4, IPv6</td>
</tr>
<tr>
<td>GUI</td>
<td>XMI Network</td>
<td>TCP: 80, TCP:443</td>
<td>IPv4, IPv6</td>
</tr>
</tbody>
</table>

Appendix F. Application VIP Failover Options (OpenStack)

Appendix F.1 Application VIP Failover Options

Within an OpenStack cloud environment, there are several options for allowing applications to manage their own virtual IP (VIP) addresses as is traditionally done in telecommunications applications. This document describes two of those options:

- Allowed address pairs
- Disable port security

Each of these options is covered in the major sub-sections that follow. The last major sub-section discusses how to utilize application managed virtual IP addresses within an OpenStack VM instance.

Both of these options effectively work around the default OpenStack Networking (Neutron) service anti-spoofing rules that ensure that a VM instance cannot send packets out a network interface with a source IP address different from the IP address Neutron has associated with the interface. In the Neutron data model, the logical notion of networks, sub-networks and network interfaces are realized as networks, subnets, and ports as shown in Figure 4:
Figure 4. Neutron High-Level Data Model

Note how a port in the Neutron data model maps to at most one VM instance where internal to the VM instance, the port is represented as an available network device such as eth0. VM instances can have multiple network interfaces in which case there are multiple Neutron ports associated with the VM instance, each with different MAC and IP addresses.

Each Neutron port by default has one MAC Address and one IPv4 or IPv6 address associated with it. The IP address associated with a port can be assigned in two ways:

- Automatically by Neutron when creating a port to fulfill an OpenStack Compute (Nova) service request to associate a network interface with a VM instance to be instantiated OR
- Manually by a cloud administrator when creating or updating a Neutron port

The anti-spoofing rules are enforced at the Neutron port level by ensuring that the source IP address of outgoing packets matches the IP address Neutron has associated with the corresponding port assigned to the VM instance. By default if the source IP address in the outgoing packet does not match the IP address associated with the corresponding Neutron port then the packet is dropped.

These anti-spoofing rules clearly create a complication for the use of application managed virtual IP addresses since Neutron is not going to know about the VIPs being applied by the application to VM instance network interfaces without some interaction between the application (or a higher level management element) and Neutron. Which is why the two options in this document either fully disable the port security measures within Neutron, including the anti-spoofing rules, or expand the set of allowable source IP addresses to include the VIPs that may be used by the application running within a VM instance.

Note that for both of the options described in the following sub-sections, there is a particular Neutron service extension or feature that must be enabled for the option to work. For one option (allowed address pairs) the required Neutron extension is enabled in most default deployments whereas for the other option (allow port security to be disabled) it is not.

Within this document when describing how to use either of these two options, there is example command line operations that interact with the OpenStack Neutron service via its command line utility, simply named neutron. However, be aware that all of the operations performed using the neutron command line
utility can also be performed through the Neutron REST APIs, see the Networking v2.0 API documentation for more information.

Appendix F.2 Allowed Address Pairs

This section describes an option that extends the set of source IP addresses that can be used in packets being sent out a VM instance’s network interface (which maps to a Neutron port). This option utilizes a Neutron capability, called the allowed-address-pairs extension, which allows an entity (cloud administrator, management element, etc.) to define additional IP addresses to be associated with a Neutron port. In this way, if an application within the VM instance sends an outgoing packet with one of those additional IP addresses, then Neutron anti-spoofing rules enforcement logic does not drop those packets. The Neutron allowed-address-pairs extension is available starting with the OpenStack Havana release.

The three sub-sections that follow describe the OpenStack configuration requirements for this option, how to use this option after a VM instance has already booted, and how to utilize this option before a VM instance has booted.

Appendix F.3 OpenStack Configuration Requirements

The Neutron allowed-address-pairs extension needs to be enabled for this option to work. For most OpenStack cloud deployments this extension should be enabled by default but to check, run the following command (after sourcing the appropriate user credentials file):

```
# neutron ext-list
```

<table>
<thead>
<tr>
<th>alias</th>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>security-group</td>
<td>security-group</td>
</tr>
<tr>
<td>l3_agent_scheduler</td>
<td>L3 Agent Scheduler</td>
</tr>
<tr>
<td>net-mtu</td>
<td>Network MTU</td>
</tr>
<tr>
<td>ext-gw-mode</td>
<td>Neutron L3 Configurable external gateway mode</td>
</tr>
<tr>
<td>binding</td>
<td>Port Binding</td>
</tr>
<tr>
<td>provider</td>
<td>Provider Network</td>
</tr>
<tr>
<td>agent</td>
<td>agent</td>
</tr>
<tr>
<td>quotas</td>
<td>Quota management support</td>
</tr>
<tr>
<td>subnet_allocation</td>
<td>Subnet Allocation</td>
</tr>
<tr>
<td>dhcp_agent_scheduler</td>
<td>DHCP Agent Scheduler</td>
</tr>
<tr>
<td>l3-ha</td>
<td>HA Router extension</td>
</tr>
<tr>
<td>multi-provider</td>
<td>Multi Provider Network</td>
</tr>
<tr>
<td>external-net</td>
<td>Neutron external network</td>
</tr>
<tr>
<td>router</td>
<td>Neutron L3 Router</td>
</tr>
<tr>
<td>allowed-address-pairs</td>
<td>Allowed Address Pairs</td>
</tr>
<tr>
<td>extraroute</td>
<td>Neutron Extra Route</td>
</tr>
<tr>
<td>extra_dhcp_opt</td>
<td>Neutron Extra DHCP opts</td>
</tr>
<tr>
<td>dvr</td>
<td>Distributed Virtual Router</td>
</tr>
</tbody>
</table>

The allowed-address-pairs extension should appear in the list of extensions as shown in the bold line above.
Appendix F.4 After a VM Instance has been Booted: Allowed Address Pairs

If a VM instance has already been booted, i.e. instantiated, and you need to associate one or more additional IP addresses with the Neutron port assigned to the VM instance then you need to execute a command of the following form:

```bash
# neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>
```

where the bolded items have the following meaning:

- **<Port ID>**
  Identifies the ID of the port within Neutron which can be determined by listing the ports, `neutron port-list`, or if the port is named then the port ID can be obtained directly in the above command with a sequence like `$(neutron port-show -f value -F id <Port Name>)` to replace the `<Port ID>` placeholder.

- **<VIP address to be added>**
  Identifies the IP address, a virtual IP address in this case, that should additionally be associated with the port where this can be a single IP address, e.g. 10.133.97.135/32, or a range of IP addresses as indicated by a value such as 10.133.97.128/30.

So for example if you wanted to indicate to Neutron that the allowed addresses for a port should include the range of addresses between 10.133.97.136 to 10.133.97.139 and the port had an ID of 8a440d3f-4e5c-4ba2-9e5e-7fc942111277 then you would type the following command:

```bash
# neutron port-update 8a440d3f-4e5c-4ba2-9e5e-7fc942111277 --allowed_address_pairs list=true type=dict ip_address=10.133.97.136/30
```

Appendix F.5 Before a VM Instance has been Booted: Allowed Address Pairs

If you want to associate additional allowed IP addresses with a port before it is associated with a VM instance then you need to first create the port and then associate one or more ports with a VM instance when it is booted. The command to create a new port with defined allowed address pairs is of the following form:

```bash
# neutron port-create --name <Port Name> --fixed-ip subnet-id=$(neutron subnet-show -f value -F id <Subnet name>),ip_address=<Target IP address> $(neutron net-show -f value -F id <Network name>) --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added>
```

where the bolded items have the following meaning:

- **<Port Name>**
  This is effectively a string alias for the port that is useful when trying to locate the ID for the port but the "--name <Port Name>" portion of the command is completely optional.

- **<Subnet name>**
  The name of the subnet to which the port should be added.

- **<Target IP address>**
  The unique IP address to be associated with the port.

- **<Network Name>**
  The name of the network with which the port should be associated.

- **<VIP address to be added>**
  This parameter value has the same meaning as described in the previous section.
So for example if you wanted to indicate to Neutron that a new port should have an IP address of 10.133.97.133 on the ‘ext-subnet’ subnet with a single allowed address pair, 10.133.97.134, then you would type a command similar to the following:

```
# neutron port-create --name foo --fixed-ip subnet-id=$(neutron subnet-show --value --F id ext-subnet),ip_address=10.133.97.133 $(neutron net-show --value --F id ext-net) --allowed_address_pairs list=true type=dict ip_address=10.133.97.134/32
```

Once the port or ports with the additional allowed addresses have been created, when you boot the VM instance use a nova boot command similar to the following:

```
# nova boot --flavor m1.xlarge --image testVMimage --nic port-id=$(neutron port-show --value --F id <Port Name>) testvm3
```

where the flavor, image, and VM instance name values need to be replaced by values appropriate for your VM. If the port to be associated with the VM instance is not named, then you need to obtain the port’s ID using the neutron port-list command and replace the `$(neutron port-show --value --F id <Port Name>)` sequence in the above command with the port’s ID value.

### Appendix F.6 Disable Port Security

This section describes an option that rather than extending the set of source IP addresses that are associated with a Neutron port, as is done with the allowed-address-pairs extension, to disable the Neutron anti-spoofing filter rules for a given port. This option allows all IP packets originating from the VM instance to be propagated no matter whether the source IP address in the packet matches the IP address associated with the Neutron port or not. This option relies upon the Neutron port security extension that is available starting with the OpenStack Kilo release.

**OpenStack Configuration Requirements**

The Neutron port security extension needs to be enabled for this method to work. For the procedure to enable the port security extension see:

**ML2 Port Security Extension Wiki page**

**Note:** Enabling the port security extension when there are already existing networks within the OpenStack cloud causes all network related requests into Neutron to fail due to a known bug in Neutron. There is a fix identified for this bug that is part of the Liberty release and is scheduled to be backported to the Kilo 2015.1.2 release. In the meantime, this option is only non-disruptive when working with a new cloud deployment where the cloud administrator can enable this feature before any networks and VM instances that use those networks are created. The port security extension can be enabled in an already deployed OpenStack cloud, but all existing networks, subnets, ports, etc., need to be deleted before enabling the port security extension. This typically means all VM instances also need to be deleted as well, but a knowledgeable cloud administrator may be able to do the following to limit the disruption of enabling the port security extension:

- Record the current IP address assignments for all VM instances,
- Remove the network interfaces from any existing VM instances,
- Delete the Neutron resources,
- Enable the port security extension,
- Re-create the previously defined Neutron resources (networks, subnets, ports, etc.), and then
- Re-add the appropriate network interfaces to the VMs.

Depending on the number of VM instances running in the cloud, this procedure may or may not be practical.
Appendix F.7  After a VM Instance has been Booted: Port Security

If you need to disable port security for a port after it has already been associated with a VM instance, then you need to execute one or both of the following commands to use the port security option. First, if the VM instance with which the existing port is associated has any associated security groups (run `nova list-secgrou <VM instance name>` to check), then you first need to run a command of the following form for each of the security group(s) associated with the VM instance:

```bash
# nova remove-secgrou <VM instance name> <Security group name>
```

where the bolded item has the following meaning:

- **<VM instance name>**
  - Identifies the name of the VM instance for which the identified security group name should be deleted.

- **<Security group name>**
  - Identifies the name of the security group that should be removed from the VM instance.

So for example if you wanted to remove the default security group from a VM instance named ‘testvm4’ then you would type a command similar to the following:

```bash
# nova remove-secgrou testvm4 default
```

Once any security groups associated with VM instance to which the Neutron port is assigned have been removed, then the Neutron port(s) associated with the target VM instance need to be updated to disable port security on those ports. The command to disable port security for a specific Neutron port is of the form:

```bash
# neutron port-update <Port ID> --port-security-enabled=false
```

where the bolded item has the following meaning:

- **<Port ID>**
  - Identifies the ID of the port within Neutron which can be determined by listing the ports, `neutron port-list`, or if the port is named then the port ID can be obtained directly in the above command with a sequence such as `$(neutron port-show -f value -F id <Port Name>)`.

So for example if you wanted to indicate to Neutron that port security should be disabled for a port with an ID of 6d48b5f2-d185-4768-b5a4-c0d1d8075e41 then you would type the following command:

```bash
# neutron port-update 6d48b5f2-d185-4768-b5a4-c0d1d8075e41 --port-security-enabled=false
```

If the port-update command succeeds, within the VM instance with which the 6d48b5f2-d185-4768-b5a4-c0d1d8075e41 port is associated, application managed VIPs can now be added to the network interface within the VM instance associated with the port and network traffic using that VIP address should now propagate.

Appendix F.8  Before a VM Instance has been Booted: Port Security

If you want to disable port security for a port before it is associated with a VM instance, then you need to first create the port at which time you can specify that port security should be disabled. The command to create a new port with port security disabled is of the following form:

```bash
# neutron port-create --name <Port Name> --port-security-enabled=false --fixed-ip subnet-id=$(neutron subnet-show -f value -F id <Subnet name>),ip_address=<Target IP address> $(neutron net-show -f value -F id <Network name>)
```
where the bolded items have the following meaning:

- **<Port Name>**
  This is effectively a string alias for the port that is useful when trying to locate the ID for the port but the "--name <Port Name>" portion of the command is completely optional.

- **<Subnet name>**
  The name of the subnet to which the port should be added.

- **<Target IP address>**
  The unique IP address to be associated with the port.

- **<Network Name>**
  The name of the network with which the port should be associated.

So for example if you wanted to indicate to Neutron that a new port should have port security disabled and an IP address of 10.133.97.133 on the 'ext-subnet' subnet then you would type a command similar to the following:

```bash
# neutron port-create --name foo --port-security-enabled=false --fixed-ip subnet-id=$(neutron subnet-show -f value -F id ext-subnet),ip_address=10.133.97.133 $(neutron net-show -f value -F id ext-net)
```

Once the port or ports with port security disabled have been created, when you boot the VM instance, you need to execute a command similar to the following:

```bash
# nova boot --flavor m1.xlarge --image testVMimage --nic port-id=$(neutron port-show -f value -F id <Port Name>) testvm3
```

where the flavor, image, and VM instance name values need to be replaced by values appropriate for your VM. If the port to be associated with the VM instance is not named, then you need to obtain the port’s ID using the neutron port-list command and replace the $(neutron port-show -f value -F id <Port Name>) sequence in the above command with the port’s ID value.

**Appendix F.9  Managing Application Virtual IP Addresses within VM Instances**

Once either of the previously described options is in place to enable applications to manage their own virtual IP addresses, there should be no modifications required to how the application already manages its VIPs in a non-virtualized configuration. There are many ways that an application can add or remove virtual IP addresses but as a reference point, here are some example command line operations to add a virtual IP address of 10.133.97.136 to the eth0 network interface within a VM and then send four gratuitous ARP packets to refresh the ARP caches of any neighboring nodes:

```bash
# ip address add 10.133.97.136/23 broadcast 10.133.97.255 dev eth0 scope global
# arping -c 4 -U -I eth0 10.133.97.136
```

As the creation of virtual IP addresses typically coincides with when an application is assigned an active role, the above operations would be performed both when an application instance first receives an initial active HA role or when an application instance transitions from a standby HA role to the active HA role.

**Appendix G.  Sample Net Rules File**

Udev uses rules files that determine how it identifies devices and creates device names. The udev daemon (udevd) reads the rules files at system startup and stores the rules in memory. If the kernel discovers a new device or an existing device goes offline, the kernel sends an event action (uevent) notification to udevd, which matches the in-memory rules against the device attributes in /sys to identify the device. As part of device event handling, rules can specify additional programs that should run to
configure a device. Rules file, which have the file extension .rules, is located in the following directory: 
/etc/udev/rules.d/*.rules

Sample File:

# eth0 interface with MAC address "fa:16:3e:cc:12:d6" will be assigned "xmi"
SUBSYSTEM="net", ACTION="add", DRIVERS="?*",
ATTR{address}="fa:16:3e:cc:12:d6", ATTR{dev_id}="0x0", ATTR{type}="1",
KERNEL="eth*", NAME="xmi"

# eth1 interface with MAC address "fa:16:3e:1a:8d:8a" will be assigned "int"
SUBSYSTEM="net", ACTION="add", DRIVERS="?*",
ATTR{address}="fa:16:3e:1a:8d:8a", ATTR{dev_id}="0x0", ATTR{type}="1",
KERNEL="eth*", NAME="int"

Note: If you need a 3rd interface add respective entry also. The iDIH Mediation VM needs an imi interface too.

Notes:
1. MAC address of each interfaces can be determined using the following command issued from the console: ifconfig -a
2. Update MAC address for each interface. The MAC addresses must be entered in all lower case.
3. Update the interface names as in the above example

Appendix H. Performance Tuning Recommended

Appendix H.1 KVM/OpenStack

For the DSR system to achieve 50K MPS or more through IPFE, a few tuning parameters need to be changed.

txqueuelen

Tuned on the compute hosts.

Purpose: default value of 500 is too small. Our recommendation is to set to 30000. Increases the network throughput of a VM.

How/what to change:

On each compute host, do the following as root.

# cat > /etc/udev/rules.d/60-tap.rules << EOF
KERNEL="tap*", RUN="/sbin/ip link set %k txqueuelen 30000"
EOF

Reload and apply to the running system

# udevadm control --reload-rules
# udevadm trigger --attr-match=subsystem=net
Ring buffer increase on the physical Ethernet interfaces
Tuned on the compute hosts.

**Purpose:** Improves the overall network throughput of the host.

**How/what to change:** This varies depending on the Host OS. The following steps are applicable to centos/fedora/rhel.

Add the following line into the network script of the interface you want to change. For example: To change the ring buffer on the eth2 interface. Edit `/etc/sysconfig/network-scripts/ifcfg-eth2` to add the `ETHTOOL_OPTS=` line as shown.

```
DEVICE=eth2
TYPE=Ethernet
ETHTOOL_OPTS="--set-ring eth2 rx 4096 tx 4096"
```

Restart the network using "service network restart" as root. Check the setting using `ethtool -g eth2`.

**Multiqueue [on IPFE]**
To be enabled on the openstack flavor and glance image for IPFE instance.

**Purpose:** Improves the network throughput of a VM.

**How/What to change:**

You need to update the flavor and the image to enable multiqueue. All guests using that image will be created with multiqueue.

```
# openstack flavor set m1.large --property hw:vif_multiqueue_enabled=true
# glance image-update b5592ed4-8f41-48a9-9f0c-e0e46cb3dd6c --property hw_vif_multiqueue_enabled=true
```

On the Guest set the number of queues to number of vcpus.

```
ethtool -L <eth interface> combined <number of vcpus>
```

**Appendix H.2   VMware**

**txqueuelen**
Tuned on the ESXi hosts.

**Purpose:** Default value of 500 is too small. The recommendation is to set to 10000 which increases the network throughput of a VM. ESXi defaults the value to 500 and permits a max value of 10000

**How/What to change:**

Log into the cli console of the ESX host and execute the below esxcli command:

```
esxcli system settings advanced set -i=10000 -o=/Net/MaxNetifTxQueueLen
```

**Ring buffer increase on the physical Ethernet interfaces**
Tuned on the ESXi hosts.

**Purpose:** Improves the overall network throughput of the host. On an ESXi host Rx buffer defaults to 512 and Tx buffer defaults to 1024 and the max value for both is 4096

**How/What to change:**

Log into the cli console of the ESX host and execute the below esxcli commands:
#esxcfg-nics -l   (lists all the physical NICs attached to the host)
#ethtool -g <interface name>   (shows the current ring buffer size)
#ethtool -G <interface name> rx 4096   (increases the rx buffer size to 4096)
#ethtool -G <interface name> tx 4096   (increases the tx buffer size to 4096)

**Multiqueue**
Already enabled on ESXi for vmxnet3 adapters.

**Purpose:** Improves the network throughput of a VM.

**Advanced NUMA settings**
Tuned on ESXi hosts.

**Purpose:** Prevents the ESXi scheduler to move VMs around from one NUMA node to another.

**How/What to change:**
Log into the cli console of the ESX host and execute the below esxcli commands:

```
#esxcli system settings advanced set -i=0 -o=/Numa/SwapLoadEnable
#esxcli system settings advanced set -i=0 -o=/Numa/SwapLocalityEnable
```

**Appendix I. My Oracle Support (MOS)**

MOS ([https://support.oracle.com](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](http://www.oracle.com/us/support/contact/index.html). When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with MOS, select 2.

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