

Oracle® Communications

Diameter Signaling Router

DSR Cloud Installation

Release 8.0

E76331-02

June 2017

ORACLE®

Oracle Communications Diameter Signaling Router Cloud Installation Procedure, Release 8.0

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: Use only the Upgrade procedure included in the Upgrade Kit.

Before upgrading any system, please access My Oracle Support (MOS) (<https://support.oracle.com>) and review any Technical Service Bulletins (TSBs) that relate to this upgrade.

My Oracle Support (MOS) (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>.

See more information on MOS in Appendix J My Oracle Support (MOS).

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 Strategy	11
3.3. SNMP Configuration	12
3.4. Installation Procedures	13
3.5. Optional Features	14
4. Software Installation Procedure	15
4.1. Create DSR Guests (VMware)	15
4.2. Create DSR Guests (KVM/OpenStack)	18
4.3. Create DSR Guests (OVM-S/OVM-M)	23
4.4. Application Configuration	36
4.5. Configure Signaling Network Routes	89
4.6. Configure DSCP (Optional)	93
4.7. Configure IP Front End (Optional)	96
4.8. SNMP Configuration (Optional)	101
4.9. Create iDIH Virtual Machines (VMware)	102
4.10. Create iDIH Virtual Machines (KVM/OpenStack)	104
4.11. Create iDIH Virtual Machines - OVM-S/OVM-M (Optional)	108
4.12. Configure iDIH Virtual Machines	119
4.13. Post iDIH Installation Configuration	121
4.14. Post-Install Activities	137
Appendix A. Sample Network Element and Hardware Profiles	145
Appendix B. List of Frequently Used Time Zones	145
Appendix C. Resource Profile	147
Appendix D. Common KVM/Openstack Tasks	149

Appendix E. Common OVM-Manager Tasks (CLI)	152
E-1. Set Up the Server	152
E-2. Create a VM	158
E-3. Server Pool	163
Appendix F. Firewall Ports	163
Appendix G. Application VIP Failover Options (OpenStack)	164
G-1. Application VIP Failover Options	164
G-2. Allowed Address Pairs	165
G-3. OpenStack Configuration Requirements	166
G-4. After a VM Instance has been Booted: Allowed Address Pairs	166
G-5. Before a VM Instance has been Booted: Allowed Address Pairs	167
G-6. Disable Port Security	167
G-7. After a VM Instance has been Booted: Port Security	168
G-8. Before a VM Instance has been Booted: Port Security	169
G-9. Managing Application Virtual IP Addresses within VM Instances	170
Appendix H. Sample Net Rules File	170
Appendix I. Performance Tuning Recommendations	171
I.1. KVM/OpenStack	171
I.2. VMWare	172
Appendix J. My Oracle Support (MOS)	173

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	145

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	145

List of Procedures

Procedure 1. (VMware) Import DSR OVA	15
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 7. (OVM-S/OVM-M) Import DSR OVA	23
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)	74
Procedure 21. Configure the MP Virtual Machines	74
Procedure 22. Configure Places and Assign MP Servers to Places (PCA and DCA Only)	83
Procedure 23. Configure the MP Server Group(s) and Profiles	84
Procedure 24. Configure the Signaling Network Routes	89
Procedure 25. Configure DSCP Values for Outgoing Traffic (Optional)	93
Procedure 26. IP Front End (IPFE) Configuration	96
Procedure 27. Configure SNMP Trap Receiver(s) (Optional)	101
Procedure 28. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)	102
Procedure 29. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)	104
Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each	108
Procedure 31. Configure iDIH VM Networks (Optional)	119
Procedure 32. Run Post Installation Scripts on iDIH VMs (Optional)	121
Procedure 33. Configure DSR Reference Data Synchronization for iDIH (Optional)	123
Procedure 34. iDIH Configuration: Configure the SSO Domain (Optional)	126
Procedure 35. Integrate iDIH into DSR (Optional)	132
Procedure 36. iDIH Configuration: Configure the Mail Server (Optional)	133
Procedure 37. iDIH Configuration: Configure SNMP Management Server (Optional)	135
Procedure 38. iDIH Configuration: Change Network Interface (Optional)	136
Procedure 39. Configure ComAgent Connections	137
Procedure 40. Complete PCA Configuration (Optional)	142
Procedure 41. Backups and Disaster Prevention	142
Procedure 42. (KVM/OpenStack Only) Configure Port Security	142

Procedure 43. Enable/Disable DTLS (SCTP Diameter Connections Only).....	144
Procedure 44. Shared Secret Encryption Key Revocation (RADIUS Only)	144
Procedure 45. DSR Performance Tuning	144
Procedure D-1. Create a Network Port	149
Procedure D-2. Create and Boot OpenStack Instance	150
Procedure D-3. Configure Networking for OpenStack Instance	151
Procedure E-1. Set Up Server	152
Procedure E-2. Create a VM.....	158

1. Introduction

1.1. Purpose and Scope

This document describes the application-related installation procedures for Diameter Signaling Router Cloud systems.

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

- [1] Communication Agent Configuration Guide, E76908
- [2] DSR PCA Activation Guide, E81528
- [3] DSR Meta Administration Feature Activation Procedure, E58661
- [4] DSR Full Address Based Resolution (FABR) Feature Activation Procedure, E78925
- [5] DSR Range Based Address Resolution (RBAR) Feature Activation, E78926
- [6] SDS SW Installation and Configuration Guide, CGBU_010592, E79531
- [7] MAP-Diameter IWF Feature Activation Procedure, E78927
- [8] Operations, Administration, and Maintenance (OAM) User's Guide, E83052
- [9] Communication Agent User's Guide, E76908
- [10] Diameter User's Guide, E76919
- [11] Mediation User's Guide, E76922
- [12] Range Based Address Resolution (RBAR) User's Guide, E76923
- [13] Full Address Based Resolution (FABR) User's Guide, E76924
- [14] IP Front End (IPFE) User's Guide, E76927
- [15] DSR Alarms and KPIs Reference, E76928
- [16] Measurements Reference, E76929
- [17] Diameter Common User's Guide, E81906
- [18] Map-Diameter IWF User's Guide, E76930
- [19] Gateway Location Application (GLA) User's Guide, E76932
- [20] DSR Security Guide, E76974
- [21] DSR IPv6 Migration Guide, E57517
- [22] DSR DTLS Feature Activation Procedure, E78942
- [23] DSR RADIUS Shared secret encryption key revocation MOP MO008572
- [24] DCA Framework and Application Activation and Deactivation Guide, E80801
- [25] Oracle VM, E64081
- [26] Networking v2.0 API documentation

1.3. Acronyms

An alphabetized list of acronyms used in the document.

Table 1. Acronyms

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

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 2. Terminology

Term	Definition
Site	<p>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.</p> <p>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.</p> <p>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.</p>
Place Association	<p>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.</p> <p>The Policy & Charging DRA application defines two place association types: policy binding region and policy & charging mated sites.</p>
Policy & Charging SBR Server Group Redundancy	<p>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.</p>
Server Group Primary Site	<p>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.</p> <p>For the Diameter custom application, these sites (places) are configured in Applications Region place association.</p> <p>The primary site may be in a different site (place) for each configured SOAM or SBR server group.</p> <p>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.</p>
Server Group Secondary Site	<p>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.</p> <p>For the Diameter custom application, these sites (places) are configured in Applications Region place association.</p> <p>The secondary site may be in a different sites (places) for each configured SOAM or SBR server group.</p> <p>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.</p>

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 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.

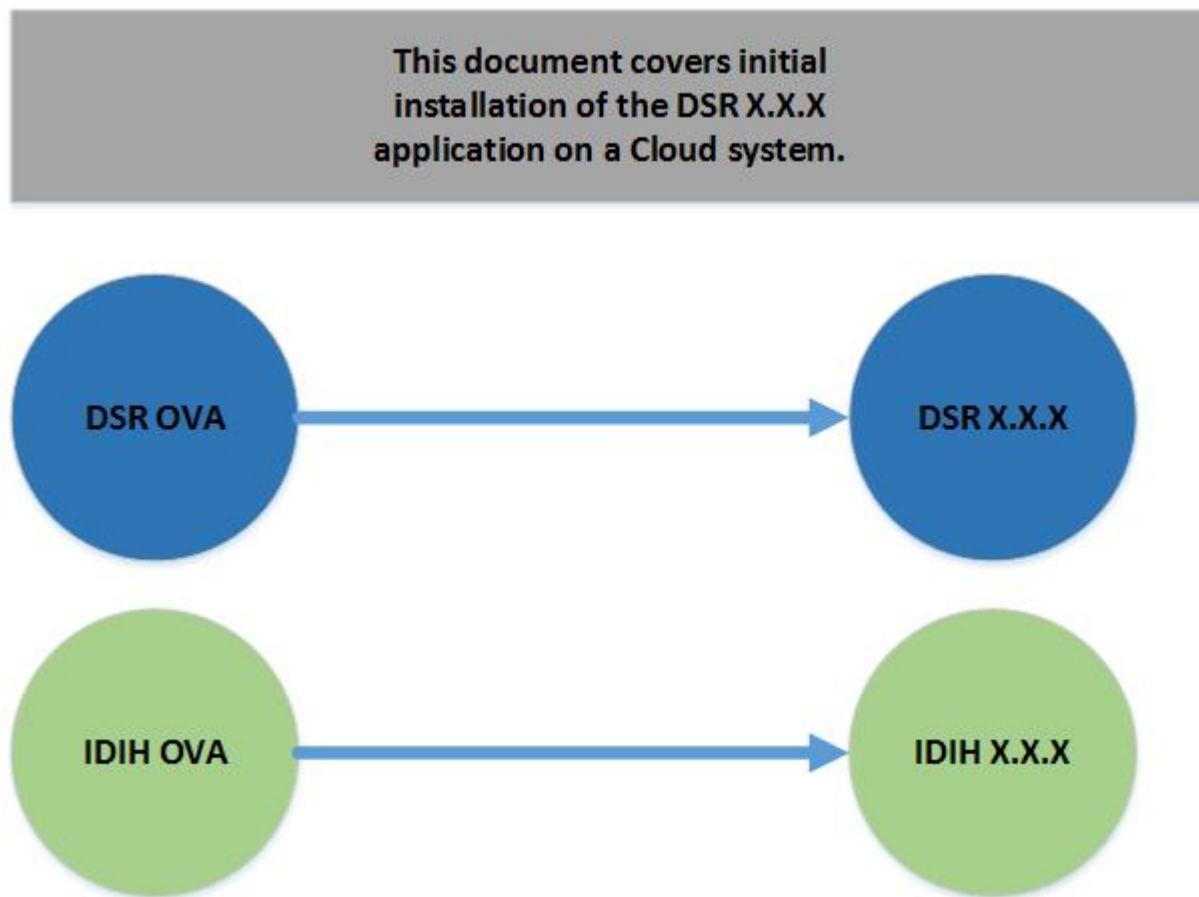


Figure 1. Initial Application Installation Path – Example shown

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.

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 Installation Strategy discusses the overall installation strategy and includes an installation flowchart to determine exactly which procedures should be run for an installation. Section 3.4 Installation Procedures 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 in Appendix F Firewall Ports. It should also be noted that some procedures are cloud platform dependent and not all procedures are performed on all cloud platforms.

3.1. 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 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: XML 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.**

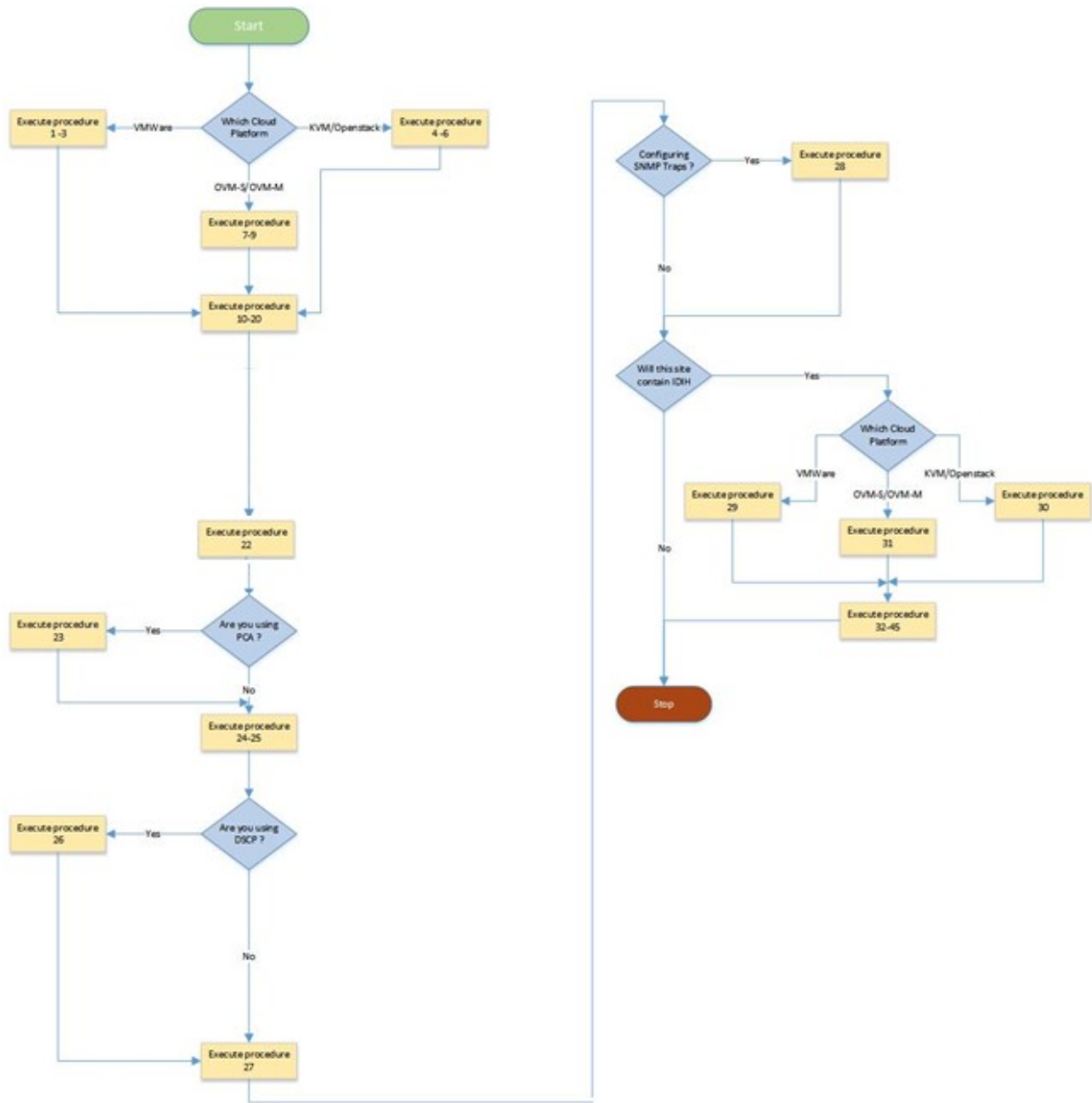


Figure 2: DSR Single Site Installation Procedure Map

3.3. 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.

DSR auxiliary components must have their SNMP trap destinations set explicitly. Trap destinations can be the NOAM VIP, the SOAM VIP, or an external (customer) NMS.

Should have their SNMP trap destinations set to:

3. The local SOAM VIP
4. The customer NMS, if available

3.4. 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

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 1 or 4 or 7	Import DSR OVA	5	5
Procedure 2 or 5 or 8	Configure DSR NOAM guest role based on resource profile	10	15
Procedure 3 or 6 or 9	Configure Remaining DSR Guests Based on Resource Profile and Configure Network	40	55
Procedure 10	Configure the NOAM Server Group	15	95
Procedure 11	Configure the Second NOAM Server	15	110
Procedure 12	Complete Configuring the NOAM Server Group	10	120
Procedure 13(Optional)	Configure the DR NOAM NE and Server	25	145
Procedure 14(Optional)	Configure the DR NOAM Server Group	15	160
Procedure 15(Optional)	Configure the Second DR NOAM Server	15	175
Procedure 16(Optional)	Complete Configuring the NOAM Server Group	10	185
Procedure 17	Configure the SOAM NE	15	200
Procedure 18	Configure the SOAM Servers	10	210
Procedure 19	Configure the SOAM Server Group	10	220
Procedure 20(Optional)	Activate PCA/DCA (PCA/DCA Only)	10	230
Procedure 21	Configure the MP Virtual Machines	5	235
Procedure 22 (Optional)	Configure Places and Assign MP Servers to Places (PCA and DCA Only)	10	245
Procedure 23	Configure the MP Server Group(s) and Profiles	10	255
Procedure 24	Configure the Signaling Networks	5	260
Procedure 25 (Optional)	Configure DSCP Values for Outgoing Traffic	10	270
Procedure 26	IP Front End (IPFE) Configuration	20	290

Procedure	Phase	Elapsed Time (Minutes)	
		This Step	Cum.
Procedure 27 (Optional)	Configure SNMP for Trap Receiver(s)	5	295
Procedure 28, 29, or 30 (Optional)	Create iDIH Oracle, Mediation and Application VMs	45	340
Procedure 31 (Optional)	Configure iDIH VM Networks	15	355
Procedure 32 (Optional)	Run Post Installation Scripts on iDIH VM's	60	415
Procedure 33 (Optional)	Configure DSR Reference Data Synchronization for iDIH	10	425
Procedure 34 (Optional)	iDIH Configuration: Configure the SSO Domain	25	450
Procedure 35 (Optional)	Integrate iDIH into DSR	30	480
Procedure 36 (Optional)	iDIH Configuration: Configure the Mail Server	10	490
Procedure 37 (Optional)	iDIH Configuration: Configure SNMP Management Server	10	500
Procedure 38 (Optional)	iDIH Configuration: Change Network Interface	10	510
Procedure 39	Configure ComAgent Connections	20	520
Procedure 40 (Optional)	Complete PCA Configuration	30	550
Procedure 41	Backups and Disaster Prevention	15	565
Procedure 42	(KVM/OpenStack only) Configure Port Security	5	570
Procedure 43	Enable/Disable DTLS (SCTP Diameter Connections Only)	15	585
Procedure 44	Shared Secret Encryption Key Revocation (RADIUS only)	10	595
Procedure 45	DSR Performance Tuning	10	605

3.5. 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, E58661-01
Full Address Based Resolution (FABR)	DSR FABR Feature Activation Procedure, E78925-01
Range Based Address Resolution (RBAR)	DSR RBAR Feature Activation, Procedure, E78926-01
MAP-Diameter Interworking (MAP-IWF)	DSR MAP-Diameter IWF Feature Activation, E78927-01
Policy and Charging Application (PCA)	Policy and Charging DRA Feature Activation Procedure, E81528-01
Host Intrusion Detection System (HIDS)	DSR Security Guide, E76974-01, Section 3.2
Diameter Custom Applications (DCA)	DCA Framework and Application Activation and Deactivation Guide, E80801

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, E57517 for instructions on how to accomplish this migration.

4.1. Create DSR Guests (VMware)

Procedure 1. (VMware) Import DSR OVA

S T E P #	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 <input type="checkbox"/>	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

S T E P #	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 <input type="checkbox"/>	Create the NOAM1 VM from the OVA image	<ol style="list-style-type: none"> 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 <input type="checkbox"/>	Configure resources for the NOAM1 VM	Configure the NOAM1 per the Appendix C Resource Profile for the DSR NOAM using the vSphere Client or vSphere Web Client .
3 <input type="checkbox"/>	Power on NOAM1	Use the vSphere Client or vSphere Web Client to power on the NOAM1 VM .
4 <input type="checkbox"/>	Configure NOAM1	<ol style="list-style-type: none"> 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. <pre>\$ sudo netAdm add --device=<ethX> --address=<IP Address in External management Network> --netmask=<Netmask> --onboot=yes --bootproto=none</pre> 4. Add the default route for ethX: <pre>\$ sudo netAdm add --route=default --gateway=<gateway address for the External management network> --device=<ethX></pre> 5. Ping the XMI gateway for network verification. <pre>\$ ping -c3 <Gateway of External Management Network></pre>
5 <input type="checkbox"/>	Configure NOAM2	Repeat steps 1 through 4 for the NOAM2 VM.

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

S T E P #	<p>This procedure adds network addresses for all VMs.</p> <p>Note: This procedure provides an example for creating an SOAM. Follow the same steps to create other guests with their respective VM names and profiles.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Create the SOAM1 VM from the OVA image	<ol style="list-style-type: none"> 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 SOAM1 VM and select the data store.
2 <input type="checkbox"/>	Configure resources for the SOAM1 VM	Configure the SOAM1 VM per the Appendix C Resource Profile for the DSR SO using the vSphere Client or vSphere Web Client . Interfaces must be added per the network interface table at the bottom of the Appendix C Resource Profile.
3 <input type="checkbox"/>	Power on SOAM1 VM	<ol style="list-style-type: none"> 1. Power on the DSR SOAM1 VM with the vSphere Client or vSphere Web Client. 2. Monitor the vApps screen's Virtual Machines tab until the DSR VM reports Powered On in the Status column.
4 <input type="checkbox"/>	Configure XMI interface	<ol style="list-style-type: none"> 1. Access the 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. <pre>\$ sudo netAdm add --device=<ethX> --address=<IP Address in External Management Network> --netmask=<Netmask> --onboot=yes --bootproto=none</pre> 4. Add the default route for ethX: <pre>\$ sudo netAdm add --route=default --gateway=<gateway address for the External management network> --device=<ethX></pre>
5 <input type="checkbox"/>	Verify network connectivity	<ol style="list-style-type: none"> 1. Access the SOAM1 VM console using the vSphere Client or vSphere web Client. 2. Login as the admusr user. 3. Ping the NOAM1. <pre>\$ ping -c3 <IP Address in External Management Network></pre>
6 <input type="checkbox"/>	Procedure overview	<p>Repeat steps 1 through 5 for the following VMs. Use unique labels for the VM names:</p> <ul style="list-style-type: none"> 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)

S T E P #	<p>This procedure adds the DSR image to the glance image catalog.</p> <p>Check off (✓) each step as it is completed. Steps with shaded boxes require user input.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Preparation	<ol style="list-style-type: none"> 1. Create instance flavors. Use the Appendix C Resource Profile values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the Admin section, or with the <code>nova flavor-create</code> command line tool. Make the flavor names as informative as possible. Since 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) represent the RAM allocation in GB, and the final three figures (060) represent the disk space in GB. 2. If using an Intel 10 Gigabit Ethernet ixgbe driver on the host nodes, note the default LRO (Large Receive Offload) option must be disabled on the host command line. See the Intel release notes for more details. This action can be performed with the following command. <pre>\$ sudo ethtool -K <ETH_DEV> lro off</pre> 3. If using IPFE Target Set addresses (TSA): <ol style="list-style-type: none"> a. Read and understand Disable Port Security in Appendix G, including the warning note. b. Enable the Neutron port security extension.
2 <input type="checkbox"/>	Add DSR OVA image	<ol style="list-style-type: none"> 1. Copy the OVA file to the OpenStack control node. <pre>\$ scp DSR-x.x.x.x.x.ova admusr@node:~</pre> 2. Log into the OpenStack control node. <pre>\$ ssh admusr@node</pre> 3. In an empty directory, unpack the OVA file using tar. <pre>\$ tar xvf DSR-x.x.x.x.x.ova</pre> 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.x-disk1.vmdk 5. Source the OpenStack admin user credentials. <pre>\$. keystone_admin</pre> 6. Select an informative name for the new image. dsr-8.0.x.x.x-original 7. Import the image using the glance utility from the command line. <pre>\$ glance image-create --name dsr-x.x.x.x.x-original --is-public true --is-protected false --progress --container-format bare --disk-format vmdk --file DSR-x.x.x.x.x-disk1.vmdk</pre> <p>This process takes about 5 minutes, depending on the underlying infrastructure.</p>

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

S T E P #	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.	
1 <input type="checkbox"/>	Name the new VM instance	<ol style="list-style-type: none"> 1. Create an informative name for the new instance: NOAM1. 2. Examine the network interface recommendations at the bottom of the Resource Profile in Appendix C.
2 <input type="checkbox"/>	Create and boot the NOAM VM instance from the glance image	<ol style="list-style-type: none"> 1. Get the following configuration values. The image ID. <pre>\$ glance image-list</pre> The flavor ID. <pre>\$ nova flavor-list</pre> The network ID(s) <pre>\$ neutron net-list</pre> An informative name for the instance. NOAM1 NOAM2 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 interface-to-network mappings described at the bottom of the Resource Profile in Appendix C. Note: IPv6 addresses should use the v6-fixed-ip argument instead of v4-fixed-ip. <pre>\$ 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></pre> 3. View the newly created instance using the nova tool. <pre>\$ nova list --all-tenants</pre> The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.

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

3 <input type="checkbox"/>	Configure NOAM VIP (Optional)	<p>Note: Refer to Allowed Address Pairs in Appendix G for more information on VIP.</p> <p>If an NOAM VIP is needed, execute the following commands:</p> <ol style="list-style-type: none"> Find the port ID associated with the NOAM instance XMI interface. <pre>\$ neutron port-list</pre> Add the VIP IP address to the address pairs list of the NOAM instance XMI interface port. <pre>\$ neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added></pre>
4 <input type="checkbox"/>	Check if interface is configured	<p>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 nova boot... command from step 2:</p> <pre>\$ ping <XMI-IP-Provided-During-Nova-Boot></pre> <p>If the ping is successful, ignore step 5 to configure the interface manually.</p>
5 <input type="checkbox"/>	Manually configure interface, if not already done (Optional)	<p>Note: If the instance is already configured with an interface and has successfully pinged (step 4), then ignore this step to configure the interface manually.</p> <ol style="list-style-type: none"> Log into the Horizon GUI as the DSR tenant user. Go to the Compute/Instances section. Click the Name field of the newly created instance. Select the Console tab. Login as the admusr user. Configure the network interfaces, conforming to the interface-to-network mappings described at the bottom of the Resource Profile in Appendix C. <pre>\$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask></pre> <pre>\$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip></pre> <p>Verify network connectivity by pinging Gateway of XMI network. <pre>\$ ping -c3 <XMI Gatewau></pre> <p>Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.</p> </p> Reboot the NOAM VM. It takes approximately 5 minutes for the VM to complete rebooting. <pre>\$ sudo init 6</pre> <p>The new VM should now be accessible via both network and Horizon consoles.</p>
6 <input type="checkbox"/>	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

S T E P #	<p>This procedure adds network addresses for all VMs.</p> <p>Note: This procedure provides an example for creating an SOAM. Follow the same steps to create other guests with their respective VM names and profiles.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Name the new VM instance	<ol style="list-style-type: none"> 1. Create an informative name for the new instance: SOAM1. 2. Examine the network interface recommendations at the bottom of Appendix C Resource Profile.
2 <input type="checkbox"/>	Create and boot the SOAM VM instance from the glance image	<ol style="list-style-type: none"> 1. Get the following configuration values. <ol style="list-style-type: none"> a. The image ID. <code>\$ glance image-list</code> b. The flavor ID. <code>\$ nova flavor-list</code> c. The network ID(s) <code>\$ neutron net-list</code> 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 interface-to-network mappings described at the bottom of the Resource Profile in Appendix C. Note: IPv6 addresses should use the v6-fixed-ip argument instead of v4-fixed-ip. <code>\$ 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></code> 3. View the newly created instance using the nova tool. <code>\$ nova list --all-tenants</code> The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.

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

3 <input type="checkbox"/>	Configure SOAM VIP (Optional)	<p>Note: Refer to Allowed Address Pairs in Appendix G for more information on VIP.</p> <p>If an SOAM VIP is needed, execute the following commands:</p> <ol style="list-style-type: none"> Find the port ID associated with the SOAM instance XMI interface. <pre>\$ neutron port-list</pre> Add the VIP IP address to the address pairs list of the SOAM instance XMI interface port. <pre>\$ neutron port-update <Port ID> --allowed_address_pairs list=true type=dict ip_address=<VIP address to be added></pre>
4 <input type="checkbox"/>	Check if interface is configured	<ol style="list-style-type: none"> 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): <pre>\$ ping <XMI-IP-Provided-During-Nova-Boot></pre> If the ping is successful, ignore step 5 to configure the interface manually.
5 <input type="checkbox"/>	Manually configure interface, if not already done (Optional)	<p>Note: If the instance is already configured with an interface and successfully pinging (step 4), then ignore this step to configure the interface manually.</p> <ol style="list-style-type: none"> Log into the Horizon GUI as the DSR tenant user. Go to the Compute/Instances section. Click the Name field of the newly created instance. Select the Console tab. Login as the admusr user. Configure the network interfaces, conforming to the interface-to-network mappings described at the bottom of the Appendix C Resource Profile. <pre>\$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask></pre> <pre>\$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip></pre> Verify network connectivity by pinging Gateway of XMI network. <pre>\$ ping -c3 <XMI Gatewau></pre> Under some circumstances, it may be necessary to configure as many as 6 or more interfaces. Reboot the SOAM VM. It takes approximately 5 minutes for the VM to complete rebooting. <pre>\$ sudo init 6</pre> <p>The new VM should now be accessible via both network and Horizon consoles.</p>

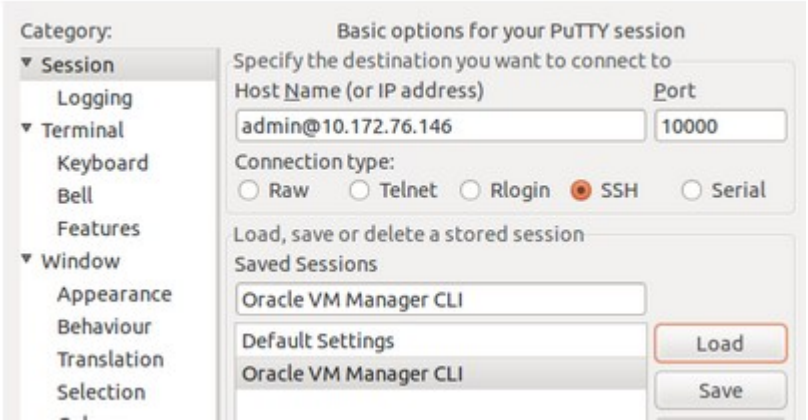
Procedure 6. (KVM/OpenStack Only) Configure Remaining DSR Guests Based on Resource Profile and Configure Network

6 <input type="checkbox"/>	Verify network connectivity	<ol style="list-style-type: none"> 1. Access the SOAM1 VM console using the openstack. 2. Login as the admusr user. 3. Ping the NOAM1. <pre>\$ ping -c3 <IP Address in External Management Network></pre>
7 <input type="checkbox"/>	Procedure overview	<p>Repeat steps 1 through 6 for the following VMs. Use unique labels for the VM names. Assign addresses to all desired network interfaces:</p> <ul style="list-style-type: none"> MP(s) MP(s) SS7 (Optional Components) IPFE(s) 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

S T E P #	<p>This procedure imports the DSR image.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>This procedure requires values for these variables:</p> <ul style="list-style-type: none"> <OVM-M IP> = IP address to access a sh prompt on the OVM server <MyRepository name> = name of the repository in the OVM to hold the product image (.ova) <URL to OVA> = link to a source for downloading the product image (.ova) <p>Executing this procedure discovers and uses the values of these variables:</p> <ul style="list-style-type: none"> <Virtual Appliance OVA ID> <OVA VM name_vm_vm> <OVM network id for (each subnet)> <OVM network name for (each subnet)> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
----------------------------------	--

Procedure 7. (OVM-S/OVM-M) Import DSR OVA

1	Access OVM command line	<p>Refer to Appendix E Common OVM-Manager Tasks (CLI) to set up the platform.</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <OVM-M IP>. <OVM-M IP> = 100.64.62.122 2. Copy and paste the value for <OVM-M IP> into the command. <pre>ssh -l admin <OVM-M IP> -p 1000</pre> For example, <code>ssh -l admin 100.64.62.221 -p 1000</code> 3. Alternatively, use a terminal emulation tool like PUTTY. 
---	-------------------------	---

Procedure 7. (OVM-S/OVM-M) Import DSR OVA

2 <input type="checkbox"/>	OVM-M CLI: Import the OVA	<p>Import the Virtual Appliance/OVA.</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <MyRepository name> and <URL to OVA>. <MyRepository name> = XLab Utility Repo01 <URL to OVA> = http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova 2. Copy and paste the values for <MyRepository name> and <URL to OVA> into the command. OVM>importVirtualAppliance Repository name='<MyRepository name>' url=<URL to OVA> Example: OVM>importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova 3. Execute the command and validate success. 4. From the screen results, find the site specific text (highlighted). Command: importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova Status: Success Time: 2017-06-19 07:33:11,777 EDT JobId: 1473420749759 Data: id: 1128a1c6ce name:DSR-8.0.0.0.0_80.23.0.ova 5. Cut and paste values for the <Virtual Appliance OVA ID>. <Virtual Appliance OVA ID> = 1128a1c6ce
-------------------------------	-------------------------------------	--

Procedure 7. (OVM-S/OVM-M) Import DSR OVA

3 <input type="checkbox"/>	OVM-M CLI: Get the virtual appliance ID, which will be used later	<ol style="list-style-type: none"> 1. Use the site-specific value for the <Virtual Appliance OVA ID>. <Virtual Appliance OVA ID> = 1128a1c6ce 2. Copy and paste the value for <Virtual Appliance OVA ID> into the command. OVM>show VirtualAppliance id=<Virtual Appliance OVA ID> Example: OVM>show VirtualAppliance id=1128a16ce 3. Execute the command and validate success. 4. From the screen results, find the site specific text (highlighted). Command: show VirtualAppliance id=1128a1c6ce Status: Success Time: 2017-04-18 15:23:53,534 EDT Data: Origin = http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.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-8.0.0.0.0_80.23.0.ova] Name = DSR-8.0.0.0.0_80.23.0.ova Description = Import URL: http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova Locked = false 5. Cut and paste values for the <OVA VM name_vm_vm>. <OVA VM name_vm_vm> = 11145510c0_vm_vm
-------------------------------	--	--

Procedure 7. (OVM-S/OVM-M) Import DSR OVA

4

OVM-M CLI:
Determine
network IDs

Find the OVM network IDs (established during the platform install).

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. Cut and paste the entire screen results, which are used in future steps.

Command: list network

Status: Success

Time: 2017-04-19 18:51:42,494 EDT

Data:

id:10486554b5 name:XSI-7 (10.196.237.0/25)

id:10f4d5744c 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:10a7289add name:Control DHCP

id:1053a604f0 name:XSI-5 (10.196.236.0/25)

id:10345112c9 name:XMI-10 (10.75.158.128/25)

4. Cut and paste values of the network ID variables (overwrite examples in table).

	OAM (XMI)	Local (IMI)	Signaling A (XSI1)	Signaling B (XSI2)	Signaling C (XSI3-16)	Replication (SBR Rep)	DIH Internal
<OVM network name>	XMI-10	IMI Shared	XSI-5	XSI-6	XSI-7	DIH Internal	XMI-10
<OVM network ID>	10345112c9	102e89a481	1053a604f0	10d8de6d9a		10486554b5	10775cf4e5

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

STEP #	<p>This procedure creates the NOAM VMs.</p> <p>Repeat this procedure for each DSR VM guest that needs to be created.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>This procedure requires values for these variables:</p> <ul style="list-style-type: none"> <OVA VM name_vm_vm> <ServerPool name> <VM name> <OVM network ID for XMI> <OVM network ID for IMI> <OVM network ID for XSI#> where # is a numeric from 1-16, for the signaling networks <OVM network ID for Replication XSI#> <URL for OVM GUI> <VM IP in XMI> from the NAPD <Gateway for XMI> from the NAPD <NetMask for XMI> from the NAPD <p>Execution of this procedure will discover and use the values of these variables:</p> <ul style="list-style-type: none"> <VM ID> <vCPUs Production> <VNIC 1 ID> <interface name> from the table in Appendix C Resource Profile. <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<p>OVM-M CLI: Create a VM for each guest</p> <p>Create a virtual machine from the virtual machine in the OVA virtual appliance.</p> <ol style="list-style-type: none"> Use the site-specific value for the <OVA VM name_vm_vm>. <OVA VM name_vm_vm> = 11145510c0_vm_vm Copy and paste the value for <OVA VM name> into the command. <pre>OVM>createVmFromVirtualApplianceVm VirtualApplianceVm name=<OVA VM name></pre> <p>Example:</p> <pre>OVM>createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm</pre> Execute the command and validate success. From the screen results, find the site specific text (highlighted). <pre>Command: createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm Status: Success Time: 2017-04-18 16:02:09,141 EDT JobId: 1492545641976 Data: id: 0004fb000000600004a0e02bdf9fc1bcd name:DSR- 8.0.0.0.0_80.23.0.ova_vm</pre> Cut and paste values for the <VM ID>. <VM ID> = 0004fb000000600004a0e02bdf9fc1bcd

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

2 <input type="checkbox"/>	OVM-M CLI: Add VM to server pool	Add the VM to server pool. <ol style="list-style-type: none"> 1. Use the site-specific value for the <VM ID> and <ServerPool name>. <VM ID> = 0004fb00000600004a0e02bdf9fc1bcd <ServerPool name> = XLab Pool 01 2. Copy and paste the values for <VM ID> and <ServerPool name> into the command. <pre>OVM>add Vm id=<VM id> to ServerPool name="<ServerPool name>"</pre> Example: <pre>OVM>add Vm id=0004fb00000600004a0e02bdf9fc1bcd to ServerPool name="XLab Pool 01"</pre> 3. Execute the command and validate success. Command: add Vm id=0004fb0000060000beeb93da703830d3c to ServerPool name="XLab Pool 01" Status: Success Time: 2017-04-19 21:05:10,950 EDT JobId: 1492650310802 Note: Refer to E-3 Server Pool for further information.
-------------------------------	--	---

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

3	<div><div></div><div>OVM-M CLI: Edit VM to apply</div></div>	<div>Edit VM with required resources:</div> <div><div>1. Use the site-specific value for the <VM ID>, <VM name>, and <vCPUs Production>.</div><div><VM id> = 0004fb00000600004a0e02bdf9fc1bcd</div><div><VM name > = na-noam-na-2a</div><div><vCPUs Production> = 4</div><div>Refer to Appendix C Resource Profile for recommended resource profile.</div></div> <div><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></div> <div><div>2. Copy and paste the values for <VM ID>, <VM name>, <vCPUs Production> into the command.</div><div>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>"</div><div>Example:</div><div>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"</div><div>3. Execute the command and validate success.</div><div>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"</div><div>Status: Success</div><div>Time: 2017-04-18 17:55:25,645 EDT</div><div>JobId: 1492552525477</div><div>The VM now has a name and resources.</div></div>	VM Name	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production	Type of guest host	#	#	#	#	#
VM Name	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production									
Type of guest host	#	#	#	#	#									
4	<div><div></div><div>OVM-M CLI: Determine VNIC ID</div></div>	<div>Identify the template VNIC on the VM.</div> <div><div>1. Use the site-specific value for the <VM name>.</div><div><VM name>= na-noam-na-2a</div><div>2. Copy and paste the values for <VM name> into the command.</div><div>OVM>show Vm name=<VM name></div><div>Example:</div><div>OVM>show Vm name=na-noam-na-2a</div><div>3. Execute the command and validate success.</div></div>												

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

	<p>4. From the screen results, find the site specific text (highlighted).</p> <pre> Command: show Vm name=NO1 Status = Stopped Memory (MB) = 6144 Max. Memory (MB) = 6144 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/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova Disk Limit = 4 Huge Pages Enabled = No Config File Absolute Path = 192.168.5.5:/storage/ovm01/repository/VirtualMachines/0004fb00000600004a0e02bdf9fc1bcd/vm.cfg Config File Mounted Path = /OVS/Repositories/0004fb0000030000da5738315337bfc7/VirtualMachines/0004fb00000600004a0e02bdf9fc1bcd/vm.cfg Server Pool = 0004fb00000200009148c8926d307f05 [XLab Pool 01] Repository = 0004fb0000030000da5738315337bfc7 [XLab Utility Repo01] Vnic 1 = 0004fb0000070000091e1ab5ae291d8a [Template Vnic] VmDiskMapping 1 = 0004fb0000130000a1996c6074d40563 [Mapping for disk Id (79def426328a4127b5bf9f7ae53d3f48.img)] VmDiskMapping 2 = 0004fb00001300002db3d4b67a143ab5 [Mapping for disk Id (EMPTY_CDROM)] Restart Action On Crash = Restart Id = 0004fb00000600004a0e02bdf9fc1bcd [na-noam-na-2a] Name = na-noam-na-2a Description = na-noam-na-2a </pre>
--	---

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

		<div>Locked = false</div> <div>DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)]</div> <div>5. Cut and paste values for the <VNIC 1 ID>.</div> <div><VNIC 1 ID> = 0004fb0000070000091e1ab5ae291d8a</div>																
5 <div></div>	Resource Profile: Determine network interfaces for the type of guest host	<div>Refer to Appendix C Resource Profile for network interfaces to configure for each guest type.</div> <table><thead><tr><th></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>Type of guest host</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> <div>Note: Create the VNICs in the correct order so the interfaces are associated with the correct network.</div>		OAM (XMI)	Local (IMI)	Sig A (XSI1)	Sig B (XSI2)	Sig C (XSI3-16)	Rep (SBR)	DIH Internal	Type of guest host	eth#	eth#	eth#	eth#	eth#	eth#	eth#
	OAM (XMI)	Local (IMI)	Sig A (XSI1)	Sig B (XSI2)	Sig C (XSI3-16)	Rep (SBR)	DIH Internal											
Type of guest host	eth#	eth#	eth#	eth#	eth#	eth#	eth#											
6 <div></div>	OVM-M CLI: Attach XMI VNIC (if needed by guest host type)	<div>Add (attach) VNIC ID of the XMI network to VM:</div> <div>1. Use the site-specific value for the <VNIC 1 ID> and <OVM Network ID for XMI>.</div> <div><VNIC 1 ID> = 004fb0000070000091e1ab5ae291d8a</div> <div><OVM Network ID for XMI> = 10345112c9</div> <div>2. Copy and paste the values for <VNIC 1 ID> and <OVM Network ID for XMI> into the command.</div> <div>OVM>add Vnic id=<VNIC 1 ID> to Network name=<OVM Network Id for XMI></div> <div>Example:</div> <div>OVM>add Vnic id=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9</div> <div>3. Execute the command and validate success.</div> <div>Command: add Vnic id=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9</div> <div>Status: Success</div> <div>Time: 2017-04-19 19:08:59,496 EDT</div> <div>JobId: 1492643339327</div>																

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

7 <input type="checkbox"/>	OVM-M CLI: Create and attach IMI VNIC (if needed by guest host type)	<p>Create VNIC ID on the IMI network and attach to VM:</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <VM name> and <OVM Network ID for IMI>. <VM name> = na-noam-na-2a <OVM Network ID for IMI> = 102e89a481 2. Copy and paste the values for <VM name> and <OVM Network ID for IMI> into the command. <pre>OVM>create Vnic network=<OVM Network ID for IMI> name=<VM name>-IMI on Vm name=<VM name></pre> Example <pre>OVM>create Vnic network=102e89a481 name=na-noam-na-2a-IMI on Vm name=na-noam-na-2a</pre> 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 Time: 2017-04-19 21:21:57,363 EDT JobId: 1492651317194 Data: id:0004fb00000700004f16dc3bfe0750a7 name:na-noam-na-2a-IMI
8 <input type="checkbox"/>	OVM-M CLI: Create and attach XSI VNIC (if needed by guest host type) Note: Repeat this step if the VM has multiple signaling networks specifying the number of networks.	<p>Create VNIC ID on the XSI network(s) and attach to VM:</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <VM name>, <OVM Network ID for XS#>, and <#>. <VM name> = hostname <OVM Network ID for XS#> = 1053a604f0 <#> = the number of the XSI network [1-16] 2. Copy and paste the values for <VM name>, <OVM Network ID for XS#>, and <#> into the command. <pre>OVM>create Vnic network=<OVM Network ID for XS#> name=<VM name>-XSI<#> on Vm name=<VM name></pre> Example: <pre>OVM>create Vnic network=1053a604f0 name=hostname-XSI1 on Vm name=hostname</pre> 3. Execute the command and validate success.

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


9 <input type="checkbox"/>	OVM-M CLI: Create and attach replication VNIC (if needed by guest host type)	<p>Create VNIC ID on the Replication network and attach to VM:</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <VM name>, <OVM Network ID for Replication XSI#>, <OVM Network Name for Replication XSI#>, and <#>. <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. Copy and paste the values for <VM name>, <OVM Network ID for Replication XSI#>, <OVM Network Name for Replication XSI#>, and <#> into the command. OVM>create Vnic network=<OVM network id for Replication XSI#> name=<VM name>-<OVM network name for Replication XSI#> on Vm name=<VM name> Example: OVM>create Vnic network=10486554b5 name= hostname-XSI7 on Vm name=hostname 3. Execute the command and validate success.
10 <input type="checkbox"/>	OVM-M CLI: Start VM	<ol style="list-style-type: none"> 1. Use the site-specific value for the <VM name>. <VM name> = na-noam-na-2a 2. Copy and paste the values for <VM name> into the command. OVM>start Vm name=<VM name> Example: OVM>start Vm name=na-noam-na-2a 3. Execute the command and validate success. Command: 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

11 <input type="checkbox"/>	OVM-M GUI: Configure networking	<p>Configure the XMI network interface for this VM:</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <URL for OVM GUI>, <interface name>, <VM IP in XMI>, <Gateway for XMI>, and <NetMask for XMI>. <p><URL for OVM GUI> = https://100.64.62.221:7002/ovm/console/faces/resource/resourceView.jspx</p> <p><interface name> = from the table in Resource Profile</p> <p><VM IP in XMI> from the NAPD</p> <p><Gateway for XMI> from the NAPD</p> <p><NetMask for XMI> from the NAPD</p> 2. Access the CLI of the console for the VM: <ol style="list-style-type: none"> a. Log into the OVM-M GUI by entering the <URL for OVM GUI> into a browser. b. Go to the servers and VMs tab. c. Expand and select the <ServerPool name>. d. From the Perspective option, select Virtual Machines. e. Select the <VM name> from the rows listed, and click the Launch Console icon. f. In the Console window, log into the VM as the admusr. 3. Copy and paste the values for <URL for OVM GUI>, <interface name>, <VM IP in XMI>, <Gateway for XMI>, and <NetMask for XMI> into the command. <p>XMI:</p> <pre>\$ 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></pre> <p>Example:</p> <pre>\$ sudo netAdm set --onboot=yes --device=eth0 -- address=10.75.158.189 --netmask=255.255.255.128</pre> <p>Example:</p> <pre>\$ sudo netAdm add --route=default --device=eth0 -- gateway=10.75.158.129</pre> 4. Execute the command and validate success. 5. Verify network connectivity by pinging the Gateway of network. <pre>\$ ping -c3 <Gateway for XMI></pre> 6. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting. <pre>\$ sudo init 6</pre> <p>The new VM is now accessible from both the network and console.</p>
--------------------------------	---	---

4.4. Application Configuration

Procedure 9. Configure the First NOAM NE and Server

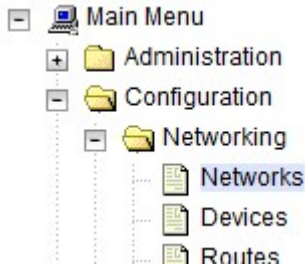
S T E P #	<p>This procedure configures the first NOAM VM.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
<p>1</p> <div style="border: 1px solid black; width: 20px; height: 20px; margin-top: 10px;"></div>	<div style="display: flex;"> <div style="flex: 1; padding-right: 10px;"> <p>NOAM GUI: Login</p> </div> <div style="flex: 4; padding-left: 10px;"> <p>Establish a GUI session as the guiadmin user on the NOAM server by using the XMI IP address.</p> <div style="text-align: center; margin-top: 20px;">  </div> <div style="margin-top: 20px;"> <p>Oracle System Login</p> <hr style="width: 50%; margin: 5px auto;"/> <div style="text-align: right; margin-top: 5px;">Mon Jul 11 13:59:37 2016 EDT</div> </div> <div style="margin-top: 20px; text-align: center;"> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 10px; width: 400px; margin: 0 auto;"> <p>Log In</p> <p>Enter your username and password to log in</p> <div style="margin-top: 10px;"> Username: <input style="width: 100%;" type="text"/> </div> <div style="margin-top: 10px;"> Password: <input style="width: 100%;" type="password"/> </div> <div style="margin-top: 10px;"> <input type="checkbox"/> Change password </div> <div style="margin-top: 10px;"> <input type="button" value="Log In"/> </div> </div> </div> <div style="margin-top: 20px; text-align: center;"> <p>Welcome to the Oracle System Login.</p> <p>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.</p> <p>Unauthorized access is prohibited.</p> </div> </div> </div>

Procedure 9. Configure the First NOAM NE and Server


2

NOAM GUI:
Create the NOAM network element using the XML file

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



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:

Browse...

zombie.xml

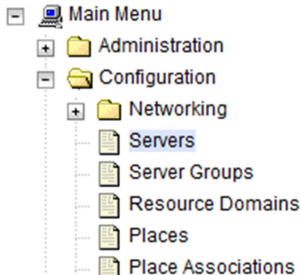
Upload File

Once the data has been uploaded, you should see a tabs appear with the name of your network element. Click on this tab which describes the individual networks that are now configured:




Global DSR_OVM_NO_NE DSR_OVM_SO_NE

Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
INTERNALXMI	OAM	Yes	Yes	Yes	6	2	10.196.227.0/24
INTERNALIMI	OAM	No	Yes	Yes	3	2	169.254.1.0/24

Procedure 9. Configure the First NOAM NE and Server

3 <input type="checkbox"/>	NOAM GUI: Map services to networks	<p>Navigate to Main Menu->Configuration->Networking->Services.</p> <p>Click Edit and set the services as shown in the table below:</p> <table border="1"> <thead> <tr> <th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr> </thead> <tbody> <tr> <td>OAM</td><td><IMI Network></td><td><XMI Network></td></tr> <tr> <td>Replication</td><td><IMI Network></td><td><XMI Network></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><IMI Network></td><td>Unspecified</td></tr> <tr> <td>ComAgent</td><td><IMI Network></td><td>Unspecified</td></tr> </tbody> </table> <p>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:</p> <table border="1"> <thead> <tr> <th>Name</th><th>Intra-NE Network</th><th>Inter-NE Network</th></tr> </thead> <tbody> <tr> <td>OAM</td><td>INTERNALIMI</td><td>INTERNALXMI</td></tr> <tr> <td>Replication</td><td>INTERNALIMI</td><td>INTERNALXMI</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>INTERNALIMI</td><td>Unspecified</td></tr> <tr> <td>ComAgent</td><td>INTERNALIMI</td><td>Unspecified</td></tr> </tbody> </table> <p>Click OK to apply the Service-to-Network selections. Dismiss any possible popup notifications.</p>	Name	Intra-NE Network	Inter-NE Network	OAM	<IMI Network>	<XMI Network>	Replication	<IMI Network>	<XMI Network>	Signaling	Unspecified	Unspecified	HA_Secondary	Unspecified	Unspecified	HA_MP_Secondary	Unspecified	Unspecified	Replication_MP	<IMI Network>	Unspecified	ComAgent	<IMI Network>	Unspecified	Name	Intra-NE Network	Inter-NE Network	OAM	INTERNALIMI	INTERNALXMI	Replication	INTERNALIMI	INTERNALXMI	Signaling	Unspecified	Unspecified	HA_Secondary	Unspecified	Unspecified	HA_MP_Secondary	Unspecified	Unspecified	Replication_MP	INTERNALIMI	Unspecified	ComAgent	INTERNALIMI	Unspecified
Name	Intra-NE Network	Inter-NE Network																																																
OAM	<IMI Network>	<XMI Network>																																																
Replication	<IMI Network>	<XMI Network>																																																
Signaling	Unspecified	Unspecified																																																
HA_Secondary	Unspecified	Unspecified																																																
HA_MP_Secondary	Unspecified	Unspecified																																																
Replication_MP	<IMI Network>	Unspecified																																																
ComAgent	<IMI Network>	Unspecified																																																
Name	Intra-NE Network	Inter-NE Network																																																
OAM	INTERNALIMI	INTERNALXMI																																																
Replication	INTERNALIMI	INTERNALXMI																																																
Signaling	Unspecified	Unspecified																																																
HA_Secondary	Unspecified	Unspecified																																																
HA_MP_Secondary	Unspecified	Unspecified																																																
Replication_MP	INTERNALIMI	Unspecified																																																
ComAgent	INTERNALIMI	Unspecified																																																
4 <input type="checkbox"/>	NOAM GUI: Insert the 1st NOAM VM	<p>Navigate to Main Menu->Configuration->Servers.</p>  <p>Click Insert to insert the new NOAM server into servers table (the first or server).</p>																																																

Procedure 9. Configure the First NOAM NE and Server

Attribute	Value
Hostname *	<input type="text"/>
Role *	- Select Role - 
System ID	<input type="text"/>
Hardware Profile	DSR Guest 
Network Element Name *	- Unassigned - 
Location	<input type="text"/>

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.]:		
Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	<input type="text" value="10.196.227.21"/>	eth0  <input type="checkbox"/> VLAN (6)
INTERNALIMI (169.254.1.0/24)	<input type="text" value="169.254.1.21"/>	eth1  <input type="checkbox"/> VLAN (3)

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

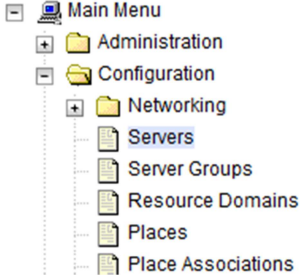
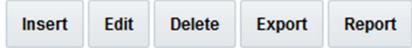
Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the **VLAN** checkbox unchecked.

Add the following NTP servers:

NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server	No
Valid NTP Server	No

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	<p>Navigate to Main Menu->Configuration->Servers.</p>  <p>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.</p> 
6	NOAM Server: Copy configuration file to 1 st NOAM server	<p>Obtain a terminal window to the 1st NOAM server, logging in as the admusr user.</p> <p>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:</p> <pre>\$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh</pre>
7	NOAM Server: Wait for configuration to complete	<p>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.</p> <p>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.</p> <p>Verify the script completed successfully by checking the following file.</p> <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Note: Ignore the warning about removing the USB key since no USB key is present. No response occurs until the reboot prompt is issued.</p>
8	NOAM Server: Set the time zone (Optional) and reboot the server	<p>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.</p> <p>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.</p> <pre>\$ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl "America/New_York" >/dev/null 2>&1 \$ sudo init 6</pre> <p>Wait for server to reboot.</p>

Procedure 9. Configure the First NOAM NE and Server

9 <input type="checkbox"/>	NOAM Server: Verify server health	Login into the NOAM1 as the admusr user. Execute the following command as admusr on the 1 st NOAM server and make sure no errors are returned: <pre> \$ 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 </pre>
-------------------------------	---	---

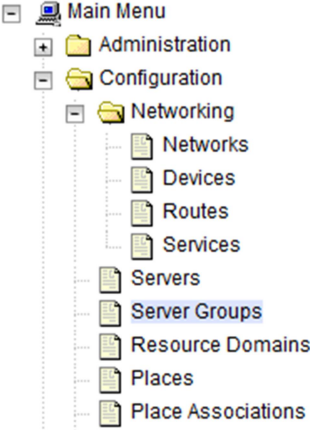

Procedure 10. Configure the NOAM Server Group

S T E P #	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 <input type="checkbox"/>	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

2	NOAM GUI: Enter NOAM server group data	<p>Navigate to Main Menu->Configuration->Server Groups.</p>  <p>Click Insert and fill in the following fields:</p> <p> Server Group Name: [Type Server Group Name] Level: A Parent: None Function: DSR (Active/Standby Pair) WAN Replication Connection Count: Use Default Value </p> <p>Adding new server group</p> <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Desc</th></tr> </thead> <tbody> <tr> <td>Server Group Name *</td><td><input type="text" value="ZombieNOAM"/></td><td>Uniqu requir</td></tr> <tr> <td>Level *</td><td><input type="text" value="A"/> ▼</td><td>Select</td></tr> <tr> <td>Parent *</td><td><input type="text" value="NONE"/> ▼</td><td>Select</td></tr> <tr> <td>Function *</td><td><input type="text" value="DSR (active/standby pair)"/> ▼</td><td>Select</td></tr> <tr> <td>WAN Replication Connection Count</td><td><input type="text" value="1"/></td><td>Speci</td></tr> </tbody> </table> <p> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </p> <p>Click OK when all fields are filled in.</p>	Field	Value	Desc	Server Group Name *	<input type="text" value="ZombieNOAM"/>	Uniqu requir	Level *	<input type="text" value="A"/> ▼	Select	Parent *	<input type="text" value="NONE"/> ▼	Select	Function *	<input type="text" value="DSR (active/standby pair)"/> ▼	Select	WAN Replication Connection Count	<input type="text" value="1"/>	Speci
Field	Value	Desc																		
Server Group Name *	<input type="text" value="ZombieNOAM"/>	Uniqu requir																		
Level *	<input type="text" value="A"/> ▼	Select																		
Parent *	<input type="text" value="NONE"/> ▼	Select																		
Function *	<input type="text" value="DSR (active/standby pair)"/> ▼	Select																		
WAN Replication Connection Count	<input type="text" value="1"/>	Speci																		

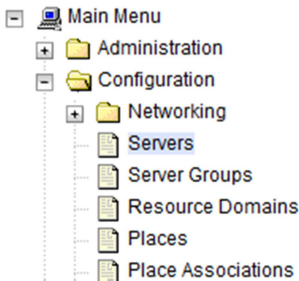
Procedure 10. Configure the NOAM Server Group

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM GUI: Edit the NOAM Server Group</p>	<p>Navigate to Main Menu->Configuration->Server Groups.</p>  <p>Select the new server group and click Edit.</p>  <p>Select the network element that represents the NOAM.</p> <table border="1" data-bbox="505 926 1398 1010"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>NO1</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> </tbody> </table> <p>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.</p> <p>Leave other boxes unchecked.</p> <p>Click OK.</p>	Server	SG Inclusion	Preferred HA Role	NO1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare
Server	SG Inclusion	Preferred HA Role						
NO1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare						
<p>4</p> <p><input type="checkbox"/></p>	<p>NOAM Server: Verify NOAM VM role</p>	<p>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.</p> <p>You might have to wait a few minutes for it to be in that state.</p> <p>Press Ctrl+C to exit.</p> <p>Example:</p> <pre data-bbox="505 1444 1398 1692">[admusr@NO1 ~]\$ ha.mystate resourceId role node DC subResources lastUpdate ----- DbReplication Act/Act A1348.092 * 0 0527:050750.672 VIP Act/Act A1348.092 * 0 0527:050750.673 CAPM_HELP_Proc Act/OOS A1348.092 * 0 0527:050750.625 DSROAM_Proc Act/OOS A1348.092 * 0 0527:050755.725 CAPM_PSFS_Proc Act/Act A1348.092 * 0 0527:050800.737 [admusr@NO1 ~]\$</pre>						

Procedure 10. Configure the NOAM Server Group

5 <input type="checkbox"/>	NOAM GUI: Restart 1 st NOAM VM	<p>From the NOAM GUI, navigate to Main Menu->Status & Manage->Server.</p>  <p>Select the first NOAM server. Click Restart.</p> <p>Click OK on the confirmation screen and wait for restart to complete.</p> 
6 <input type="checkbox"/>	NOAM Server: Set sysmetric thresholds for VMs. Note: These commands disable the message rate threshold alarms	<p>From console window of the first NOAM VM, execute the iset commands as admusr.</p> <pre> \$ 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'" </pre>

Procedure 11. Configure the Second NOAM Server

S T E P #	<p>This procedure configures the second NOAM server.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>														
1 <input type="checkbox"/>	<p>NOAM GUI: Login</p> <p>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.</p> <p>Login as the guiadmin user.</p>														
2 <input type="checkbox"/>	<p>NOAM GUI: Insert the 2nd NOAM VM</p> <p>Navigate to Main Menu->Configuration->Servers.</p>  <p>Click Insert to insert the new NOAM server into servers table (the first or server).</p> <table border="1" data-bbox="506 989 1403 1577"> <thead> <tr> <th>Attribute</th><th>Value</th></tr> </thead> <tbody> <tr> <td>Hostname *</td><td><input type="text"/></td></tr> <tr> <td>Role *</td><td>- Select Role - <input type="button" value="v"/></td></tr> <tr> <td>System ID</td><td><input type="text"/></td></tr> <tr> <td>Hardware Profile</td><td>DSR Guest <input type="button" value="v"/></td></tr> <tr> <td>Network Element Name *</td><td>- Unassigned - <input type="button" value="v"/></td></tr> <tr> <td>Location</td><td><input type="text"/></td></tr> </tbody> </table> <p>Fill in the fields as follows:</p> <p> Hostname: <Hostname> Role: NETWORK OAM&P System ID: <Site System ID> Hardware Profile: DSR Guest Network Element Name: [Choose NE list] </p> <p>The network interface fields are now available with selection choices based on the chosen hardware profile and network element.</p>	Attribute	Value	Hostname *	<input type="text"/>	Role *	- Select Role - <input type="button" value="v"/>	System ID	<input type="text"/>	Hardware Profile	DSR Guest <input type="button" value="v"/>	Network Element Name *	- Unassigned - <input type="button" value="v"/>	Location	<input type="text"/>
Attribute	Value														
Hostname *	<input type="text"/>														
Role *	- Select Role - <input type="button" value="v"/>														
System ID	<input type="text"/>														
Hardware Profile	DSR Guest <input type="button" value="v"/>														
Network Element Name *	- Unassigned - <input type="button" value="v"/>														
Location	<input type="text"/>														

Procedure 11. Configure the Second NOAM Server

		<div>OAM Interfaces [At least one interface is required.]:</div> <table><thead><tr><th>Network</th><th>IP Address</th><th>Interface</th></tr></thead><tbody><tr><td>INTERNALXMI (10.196.227.0/24)</td><td>10.196.227.21</td><td>eth0 <input type="checkbox"/> VLAN (6)</td></tr><tr><td>INTERNALIMI (169.254.1.0/24)</td><td>169.254.1.21</td><td>eth1 <input type="checkbox"/> VLAN (3)</td></tr></tbody></table> <div><div>Ok</div><div>Apply</div><div>Cancel</div></div> <p>Fill in the server IP addresses for the XMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.</p> <p>Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the VLAN checkbox unmarked.</p> <p>Add the following NTP servers:</p> <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> <p>Click OK when you have completed entering all the server data.</p>	Network	IP Address	Interface	INTERNALXMI (10.196.227.0/24)	10.196.227.21	eth0 <input type="checkbox"/> VLAN (6)	INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 <input type="checkbox"/> VLAN (3)	NTP Server	Preferred?	Valid NTP Server	Yes	Valid NTP Server	No	Valid NTP Server	No
Network	IP Address	Interface																	
INTERNALXMI (10.196.227.0/24)	10.196.227.21	eth0 <input type="checkbox"/> VLAN (6)																	
INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 <input type="checkbox"/> VLAN (3)																	
NTP Server	Preferred?																		
Valid NTP Server	Yes																		
Valid NTP Server	No																		
Valid NTP Server	No																		
3	<div><input type="checkbox"/></div> <div>NOAM GUI: Export the initial configuration</div>	<p>Navigate to Main Menu->Configuration->Servers.</p> <div><div><div><div></div><div>Main Menu</div></div><div><div></div><div>Administration</div></div><div><div></div><div>Configuration</div></div><div><div></div><div>Networking</div></div><div><div></div><div>Servers</div></div><div><div></div><div>Server Groups</div></div><div><div></div><div>Resource Domains</div></div><div><div></div><div>Places</div></div><div><div></div><div>Place Associations</div></div></div></div> <p>From the GUI screen, select the 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.</p> <div><div>Insert</div><div>Edit</div><div>Delete</div><div>Export</div><div>Report</div></div>																	
4	<div><input type="checkbox"/></div> <div>First NOAM Server: Copy configuration file to 2nd NOAM server</div>	<p>Obtain a terminal session to the 1st NOAM as the admusr user.</p> <p>Login as the admusr user to the NO1 shell and issue the following commands:</p> <pre>\$ sudo scp /var/TKLC/db/filemgmt/TKLCCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCCConfigData.sh</pre> <p>Note: ipaddr is the IP address of NOAM2 assigned to its ethx interface associated with the xmi network.</p>																	

Procedure 11. Configure the Second NOAM Server

5 <input type="checkbox"/>	Second NOAM Server: Wait for configuration to complete	<p>Obtain a terminal session to the 2nd NOAM as the admusr user.</p> <p>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.</p> <p>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.</p> <p>Verify script completed successfully by checking the following file.</p> <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Note: Ignore the warning about removing the USB key since no USB key is present.</p>
6 <input type="checkbox"/>	Second NOAM Server: Reboot the server	<p>Obtain a terminal session to the 2nd NOAM as the admusr user.</p> <pre>\$ sudo init 6</pre> <p>Wait for server to reboot.</p>
7 <input type="checkbox"/>	Second NOAM Server: Verify server health	<p>Log into the NOAM2 as admusr and wait.</p> <p>Execute the following command as super-user on the 2nd NO server and make sure no errors are returned:</p> <pre>\$ sudo syscheck</pre> <pre>Running modules in class hardware... OK</pre> <pre>Running modules in class disk... OK</pre> <pre>Running modules in class net... OK</pre> <pre>Running modules in class system... OK</pre> <pre>Running modules in class proc... OK</pre> <pre>LOG LOCATION: /var/TKLC/log/syscheck/fail_log</pre>

Procedure 12. Complete Configuring the NOAM Server Group

STEP#

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.

1

☐

NOAM GUI: Edit the NOAM Server Group Data

From the GUI session on the first NOAM server, navigate to **Main Menu->Configuration->Server Groups**.

Main Menu

Administration

Configuration

Networking

Servers

Server Groups

Resource Domains

Places

Place Associations

Select the NOAM server group and click **Edit**.

Insert

Edit

Delete

Report

Add the second NOAM server to the server group by marking the **Include in SG** checkbox for the second NOAM server. Click **Apply**.

Server	SG Inclusion	Preferred HA Role
NO1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare
NO2	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare

Click **Add** to add a NOAM VIP. Type the VIP Address and click **OK**.

VIP Assignment

VIP Address

Add

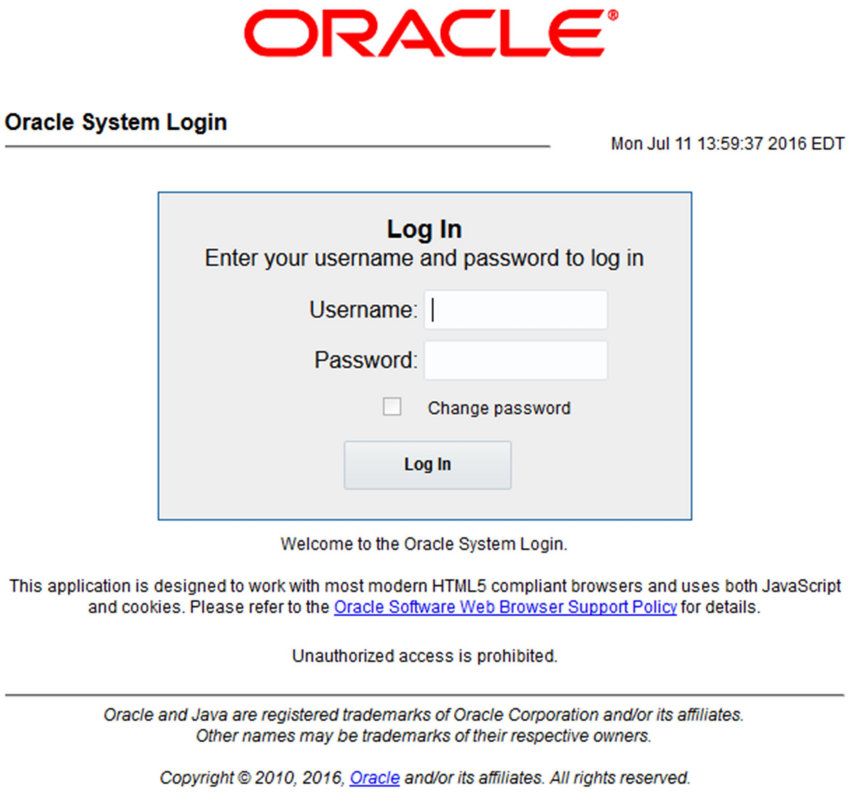
Remove

Ok

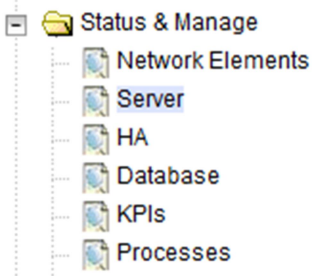
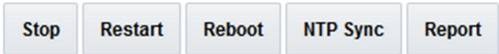
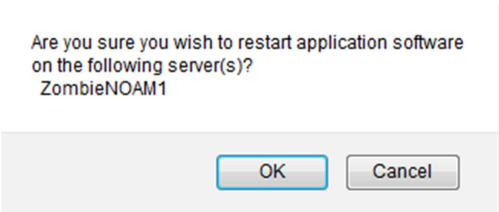
Apply

Cancel


Procedure 12. Complete Configuring the NOAM Server Group

2 <input type="checkbox"/>	Establish GUI session on the NOAM VIP	<p>Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the guiadmin user.</p> 
3 <input type="checkbox"/>	Wait for remote database alarm to clear	Wait for the alarm ID 10200 Remote Database re-initialization in progress to be cleared before proceeding (Main Menu->Alarms & Events->View Active).

Procedure 12. Complete Configuring the NOAM Server Group

4 <input type="checkbox"/>	NOAM GUI: Restart 2 nd NOAM VM	<p>Navigate to Main Menu->Status & Manage->Server and select the second NOAM server.</p>  <p>Click Restart.</p>  <p>Click OK on the confirmation screen.</p>  <p>Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the Appl State as Enabled.</p>
5 <input type="checkbox"/>	SDS can now be installed (Optional)	If this deployment contains SDS, SDS can now be installed. Refer to document referenced in [6] SDS SW Installation and Configuration Guide, CGBU_010592, E79531.

Procedure 13. Configure the DR NOAM NE and Server (Optional)

S T E P #		<p>This procedure will provide the steps to configure the first DR NOAM VM.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	Primary NOAM VIP GUI: Login	<p>Establish a GUI session on the primary NOAM server by using the XMI VIP IP address.</p> 

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

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

Main Menu

Administration

Configuration

Networking

Networks

Devices

Routes

Services

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

port

Insert Network Element

Export

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

Browse...

No file selected.

Upload File

Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

Click **Upload File** to upload the XML file.

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

Browse...

zombie.xml

Upload File

See the examples in Appendix A Sample Network Element and Hardware Profiles and configure the NOAM network element.

Once the data has been uploaded, you should see a tabs appear with the name of your network element. Click on this tab, which describes the individual networks that are now configured:

Global

DSR_OVM_NO_NE

DSR_OVM_SO_NE

Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
INTERNALXMI	OAM	Yes	Yes	Yes	6	2	10.196.227.0/24
INTERNALIMI	OAM	No	Yes	Yes	3	2	169.254.1.0/24

3

Primary NOAM VIP GUI: Insert the 1st DR NOAM VM

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

Main Menu

Administration

Configuration

Networking

Servers

Server Groups




Resource Domains

Places

Place Associations

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)

Attribute	Value
Hostname *	<input type="text"/>
Role *	- Select Role - 
System ID	<input type="text"/>
Hardware Profile	DSR Guest 
Network Element Name *	- Unassigned - 
Location	<input type="text"/>

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.]:		
Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	<input type="text" value="10.196.227.21"/>	eth0  <input type="checkbox"/> VLAN (6)
INTERNALIMI (169.254.1.0/24)	<input type="text" value="169.254.1.21"/>	eth1  <input type="checkbox"/> VLAN (3)

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

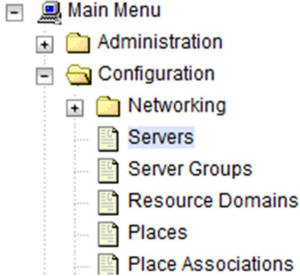
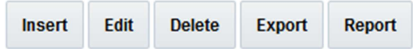
Fill in the server IP addresses for the IMI network. Select ethX for the interface. Leave the **VLAN** checkbox unchecked.

Add the following NTP servers:

NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server	No
Valid NTP Server	No

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

Procedure 13. Configure the DR NOAM NE and Server (Optional)

4	<input type="checkbox"/> Primary NOAM VIP GUI: Export the initial configuration	<p>Navigate to Main Menu->Configuration->Networking->Servers.</p>  <p>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.</p> 
5	<input type="checkbox"/> Primary NOAM Server: Copy configuration file to 1 st NOAM server	<p>Obtain a terminal window to the Primary NOAM server, logging in as the admusr user.</p> <p>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:</p> <pre>\$ sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh /var/tmp/TKLCConfigData.sh</pre>
6	<input type="checkbox"/> First DR NOAM Server: Wait for configuration to complete	<p>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.</p> <p>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.</p> <p>Verify the script completed successfully by checking the following file.</p> <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Note: Ignore the warning about removing the USB key since no USB key is present. No response occurs until the reboot prompt is issued.</p>
7	<input type="checkbox"/> First DR NOAM Server: Reboot the server	<p>Obtain a terminal window to the 1st DR NOAM server, logging in as the admusr user.</p> <pre>\$ sudo init 6</pre> <p>Wait for server to reboot.</p>

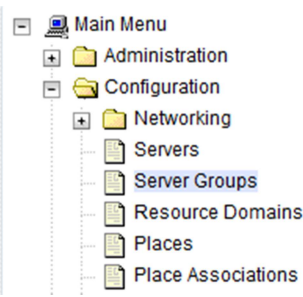
Procedure 13. Configure the DR NOAM NE and Server (Optional)

8 <input type="checkbox"/>	First DR NOAM Server: Verify server health	<p>Obtain a terminal window to the 1st DR NOAM server, logging in as the admusr user.</p> <p>Execute the following command as admusr and make sure that no errors are returned:</p> <pre>\$ 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</pre>
-------------------------------	---	---

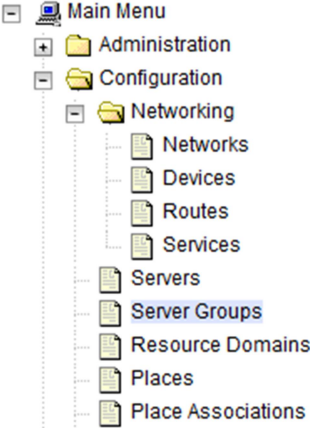
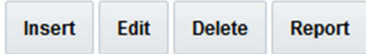
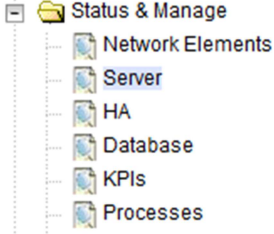
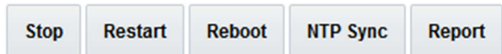
Procedure 14. Configure the DR NOAM Server Group (Optional)

S T E P #	<p>This procedure configures the DR NOAM server group.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Primary NOAM VIP GUI: Login	<p>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 http://<NO1_XMI_IP_Address> as the URL.</p> <p>Login as the guiadmin user. If prompted by a security warning, click Continue to this Website to proceed.</p>

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

2	Primary NOAM VIP GUI: Enter DR NOAM server group data	<p>Using the GUI session on the primary NOAM server, navigate to Main Menu->Configuration->Server Groups.</p>  <p>Click Insert and fill in the following fields:</p> <p>Server Group Name: [Type Server Group Name] Level: A Parent: None Function: DSR (Active/Standby Pair) WAN Replication Connection Count: Use Default Value</p> <p>Adding new server group</p> <table border="1"><thead><tr><th>Field</th><th>Value</th><th>Desc</th></tr></thead><tbody><tr><td>Server Group Name *</td><td><input type="text" value="ZombieNOAM"/></td><td>Uniqu requir</td></tr><tr><td>Level *</td><td><input type="text" value="A"/></td><td>Selec</td></tr><tr><td>Parent *</td><td><input type="text" value="NONE"/></td><td>Selec</td></tr><tr><td>Function *</td><td><input type="text" value="DSR (active/standby pair)"/></td><td>Selec</td></tr><tr><td>WAN Replication Connection Count</td><td><input type="text" value="1"/></td><td>Speci</td></tr></tbody></table> <p><input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/></p> <p>Click OK when all fields are filled in.</p>	Field	Value	Desc	Server Group Name *	<input type="text" value="ZombieNOAM"/>	Uniqu requir	Level *	<input type="text" value="A"/>	Selec	Parent *	<input type="text" value="NONE"/>	Selec	Function *	<input type="text" value="DSR (active/standby pair)"/>	Selec	WAN Replication Connection Count	<input type="text" value="1"/>	Speci
Field	Value	Desc																		
Server Group Name *	<input type="text" value="ZombieNOAM"/>	Uniqu requir																		
Level *	<input type="text" value="A"/>	Selec																		
Parent *	<input type="text" value="NONE"/>	Selec																		
Function *	<input type="text" value="DSR (active/standby pair)"/>	Selec																		
WAN Replication Connection Count	<input type="text" value="1"/>	Speci																		

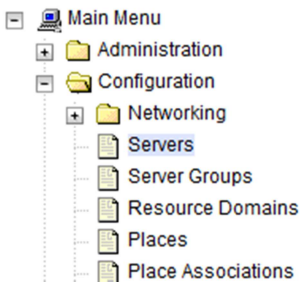
Procedure 14. Configure the DR NOAM Server Group (Optional)

3 <input type="checkbox"/>	Primary NOAM VIP GUI: Edit the DR NOAM server group	<p>Navigate to Main Menu->Configuration->Server Groups.</p>  <p>Select the new server group and click Edit.</p>  <p>Select the network element that represents the DR NOAM.</p> <table border="1" data-bbox="500 913 1399 1045"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>DSRDRNO1</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> </tbody> </table> <p>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.</p> <p>Leave other boxes unchecked.</p> <p>Click OK.</p>	Server	SG Inclusion	Preferred HA Role	DSRDRNO1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare
Server	SG Inclusion	Preferred HA Role						
DSRDRNO1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare						
4 <input type="checkbox"/>	Primary NOAM VIP GUI: Restart 1 st DR NOAM VM	<p>From the NOAM GUI, navigate to Main Menu->Status & Manage->Server.</p>  <p>Select the first NOAM server. Click Restart.</p>  <p>Click OK on the confirmation screen and wait for restart to complete.</p> <div data-bbox="500 1701 928 1885"> <p>Are you sure you wish to restart application software on the following server(s)? ZombieNOAM1</p> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div>						




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

5 <input type="checkbox"/>	NOAM Server: Set sysmetric 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 . <pre> \$ 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'" </pre>
-------------------------------	---	--

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

S T E P #	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.	
1 <input type="checkbox"/>	Primary NOAM VIP GUI: Login	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://<NOAM1_XMI_IP_Address> as the URL. Login as the guiadmin user.
2 <input type="checkbox"/>	Primary NOAM VIP GUI: Insert the 2nd DR NOAM VM	Navigate to Main Menu -> Configuration -> Networking->Servers .  Click Insert to insert the new NOAM server into servers table (the first or second server).



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

Attribute	Value
Hostname *	<input type="text"/>
Role *	- Select Role - 
System ID	<input type="text"/>
Hardware Profile	DSR Guest 
Network Element Name *	- Unassigned - 
Location	<input type="text"/>

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.

OAM Interfaces [At least one interface is required.]:		
Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	<input type="text" value="10.196.227.21"/>	eth0  <input type="checkbox"/> VLAN (6)
INTERNALIMI (169.254.1.0/24)	<input type="text" value="169.254.1.21"/>	eth1  <input type="checkbox"/> VLAN (3)

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

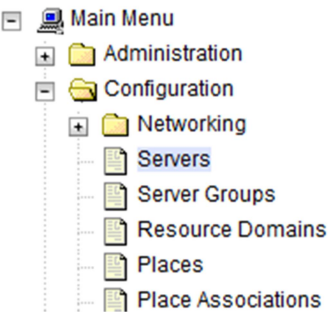
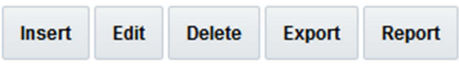
Fill in the server IP addresses for the IMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unmarked.

Add the following NTP servers:

NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server	No
Valid NTP Server	No

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

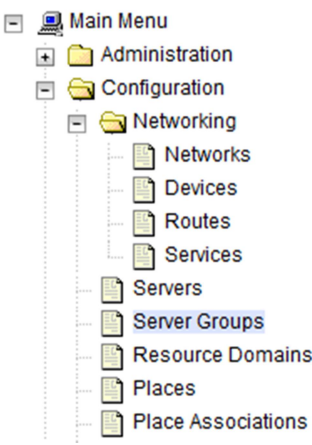


Procedure 15. Configure the Second DR NOAM Server (Optional)

3 <input type="checkbox"/>	Primary NOAM VIP GUI: Export the initial configuration	<p>Navigate to Main Menu->Configuration->Networking->Servers.</p>  <p>From the GUI screen, select the server just configured and click Export to generate the initial configuration data for that server.</p>  <p>Go to the Info tab to confirm the file has been created.</p>
4 <input type="checkbox"/>	Primary NOAM: Copy configuration file to 2 nd DR NOAM server	<p>Obtain a terminal session to the primary NOAM as the admusr user.</p> <p>Login as the admusr user to the NOAM1 shell and issue the following commands:</p> <pre>\$ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh</pre> <p>Note: ipaddr is the IP address of DR NOAM assigned to its ethx interface associated with the XML network.</p>
5 <input type="checkbox"/>	Second DR NOAM Server: Wait for configuration to complete	<p>Obtain a terminal session to the 2nd DR NOAM as the admusr user.</p> <p>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.</p> <p>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.</p> <p>Verify script completed successfully by checking the following file.</p> <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Note: Ignore the warning about removing the USB key since no USB key is present.</p>
6 <input type="checkbox"/>	Second DR NOAM Server: Reboot the server	<p>Obtain a terminal session to the 2nd DR NOAM as the admusr user.</p> <pre>\$ sudo init 6</pre> <p>Wait for server to reboot.</p>


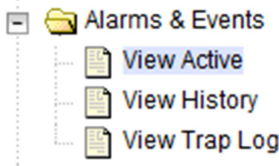
Procedure 15. Configure the Second DR NOAM Server (Optional)

7 <input type="checkbox"/>	Second DR NOAM Server: Verify server health	<p>Obtain a terminal session to the 2nd DR NOAM as the admusr user.</p> <p>Execute the following command as super-user and make sure no errors are returned:</p> <pre>\$ 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</pre>
-------------------------------	--	---

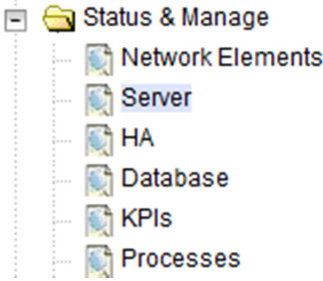
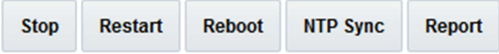
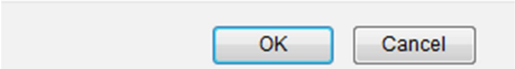
Procedure 16. Complete Configuring the DR NOAM Server Group (Optional)

S T E P #	<p>This procedure finishes configuring the DR NOAM Server Group.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>										
1 <input type="checkbox"/>	<p>PRIMARY NOAM VIP GUI: Edit the DR NOAM server group data</p>	<p>From the GUI session on the primary NOAM server, navigate to Main Menu->Configuration->Server Groups.</p>  <p>Select the NOAM server group and click Edit.</p>  <p>Add the second NOAM server to the server group by marking the Include in SG checkbox for the second NOAM server. Click Apply.</p> <table border="1" data-bbox="503 1144 1396 1281"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>DSRDRN01</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> <tr> <td>DSRDRN02</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> </tbody> </table> <p>Click Add to add an NOAM VIP. Type the VIP Address and click OK.</p> 	Server	SG Inclusion	Preferred HA Role	DSRDRN01	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare	DSRDRN02	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
DSRDRN01	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare									
DSRDRN02	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare									


Procedure 16. Complete Configuring the DR NOAM Server Group (Optional)

2 <input type="checkbox"/>	Primary NOAM VIP GUI: Establish GUI Session on the NOAM VIP	<p>Establish a GUI session on the primary NOAM by using the NOAM VIP address. Login as the guiadmin user.</p> 
3 <input type="checkbox"/>	Primary NOAM VIP GUI: Wait for Remote Database Alarm to Clear	<p>Wait for the alarm ID 10200 Remote Database re-initialization in progress to be cleared before proceeding (Main menu->Alarms & Events->View Active).</p> 

Procedure 16. Complete Configuring the DR NOAM Server Group (Optional)

4 <input type="checkbox"/>	Primary NOAM VIP GUI: Restart 2 nd DR NOAM VM	<p>Navigate to Main Menu->Status & Manage->Server and select the second DR NOAM server.</p>  <p>Click Restart.</p>  <p>Answer OK to the confirmation popup.</p> <p>Are you sure you wish to restart application software on the following server(s)? ZombieNOAM2</p>  <p>Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the Appl State as Enabled.</p>						
5 <input type="checkbox"/>	Primary NOAM: Modify DSR OAM process	<p>Establish an SSH session to the primary NOAM, login as the admusr user. Execute the following commands:</p> <ol style="list-style-type: none"> Retrieve the cluster ID of the DR-NOAM: <pre>\$ sudo iqt -fClusterID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>'"</pre> <table border="1"> <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> Execute the following command to start the DSR OAM process on the DR-NOAM. <pre>\$ echo "<clusterID> DSROAM_Proc Yes" iload -ha -xun -fcluster -fresource -foptional HaClusterResourceCfg</pre> 	Server_ID	NodeID	ClusterID	1	Oahu-DSR-DR-NOAM-2	A1055
Server_ID	NodeID	ClusterID						
1	Oahu-DSR-DR-NOAM-2	A1055						

Procedure 17. Configure the SOAM NE

S T E P #	<p>This procedure configures the SOAM network element.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
<p>1</p> <p><input type="checkbox"/></p>	<div> <div> <p>Primary NOAM VIP GUI:</p> <p>Establish GUI session on the NOAM VIP</p> </div> <div> <p>If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the guiadmin user.</p>  </div> </div>

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

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

A screenshot of a web application's navigation menu. The menu is structured as a tree. At the top is 'Main Menu' with a computer icon. Below it is 'Administration' with a folder icon. Under 'Administration' is 'Configuration' with a folder icon. Under 'Configuration' is 'Networking' with a folder icon. Under 'Networking' are four items: 'Networks' (document icon, highlighted with a blue background), 'Devices' (document icon), 'Routes' (document icon), and 'Services' (document icon).

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

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

zombieSOAM.xml

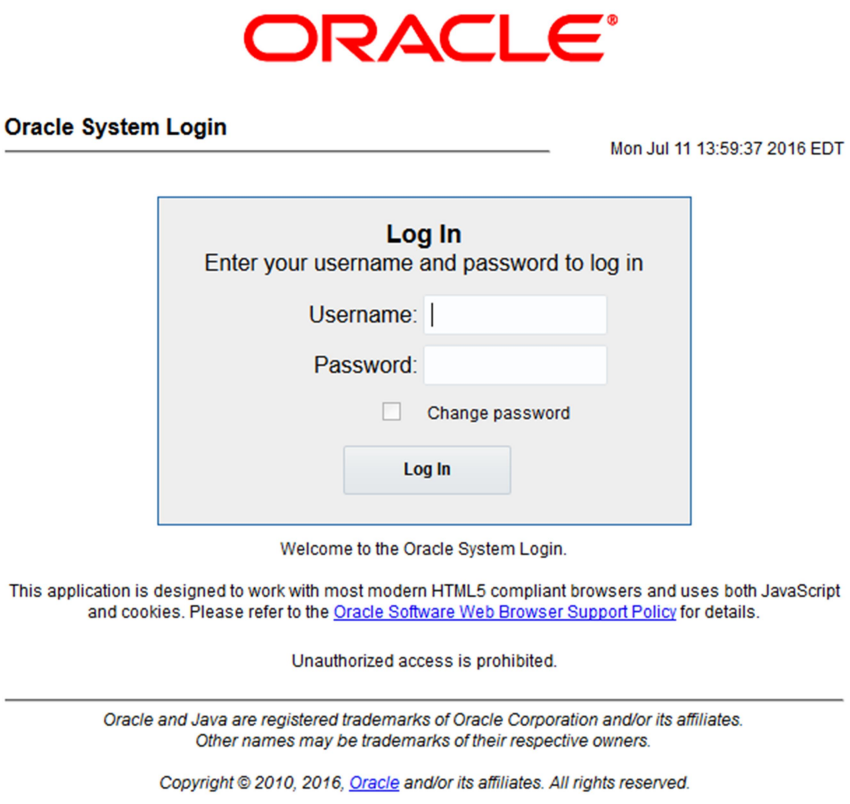
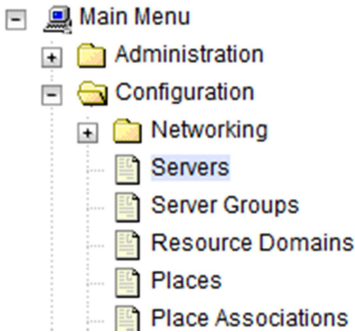
Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.

Click **Upload** to upload the XML file and configure the SOAM network element.




A screenshot of a web application's configuration page. At the top, there are four tabs: 'Global', 'ZombieNOAM', 'ZombieDRNOAM', and 'ZombieSOAM' (which is selected and highlighted with a blue border). Below the tabs is a table with the following data:

Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
XMI	OAM	Yes	Yes	Yes	4	0	10.240.213.0/24
IMI	OAM	No	Yes	No	3	0	169.254.1.0/24

Procedure 18. Configure the SOAM Servers

S T E P #	<p>This procedure configures the SOAM servers.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
<p>1</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI:</p> <p>Establish GUI session on the NOAM VIP</p>	<p>If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the guiadmin user.</p> 
<p>2</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Insert the 1st SOAM server</p>	<p>Navigate to Main Menu->Configuration->Servers.</p>  <p>Click Insert to insert the new SOAM server into servers table.</p>



Procedure 18. Configure the SOAM Servers

Attribute	Value
Hostname *	<input type="text"/>
Role *	- Select Role - 
System ID	<input type="text"/>
Hardware Profile	DSR Guest 
Network Element Name *	- Unassigned - 
Location	<input type="text"/>

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.

OAM Interfaces [At least one interface is required.]:		
Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	<input type="text" value="10.196.227.23"/>	eth0  <input type="checkbox"/> VLAN (6)
INTERNALIMI (169.254.1.0/24)	<input type="text" value="169.254.1.23"/>	eth1  <input type="checkbox"/> VLAN (3)

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

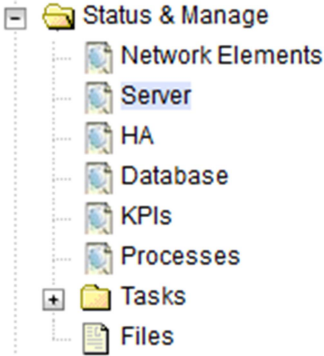
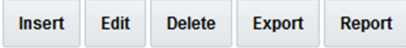
Fill in the server IP addresses for the IMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unmarked.

Add the following NTP servers:

NTP Server	Preferred?
Valid NTP Server	Yes
Valid NTP Server	No
Valid NTP Server	No

Click **OK** when you have completed entering the server data.

Procedure 18. Configure the SOAM Servers

3 <input type="checkbox"/>	Primary NOAM VIP GUI: Export the initial configuration	<p>Navigate to Main Menu->Status & Manage->Server.</p>  <p>From the GUI screen, select the desired server and click Export to generate the initial configuration data for that server.</p>  <p>Go to the Info tab to confirm the file has been created.</p>
4 <input type="checkbox"/>	Primary NOAM: Copy configuration file to the 1 st SOAM server	<p>Log in as the admusr user to the NOAM1 shell and issue the commands:</p> <pre>\$ sudo scp /var/TKLC/db/filemgmt/TKLCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCConfigData.sh</pre>
5 <input type="checkbox"/>	First SOAM Server: Wait for configuration to complete	<p>Obtain a terminal session on the 1st SOAM as the admusr user.</p> <p>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.</p> <p>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.</p> <p>Verify script completed successfully by checking the following file.</p> <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Note: Ignore the warning about removing the USB key since no USB key is present.</p>
6 <input type="checkbox"/>	First SOAM Server: Reboot the server	<p>Obtain a terminal session to the 1st SOAM as the admusr user.</p> <pre>\$ sudo init 6</pre> <p>Wait for server to reboot.</p>

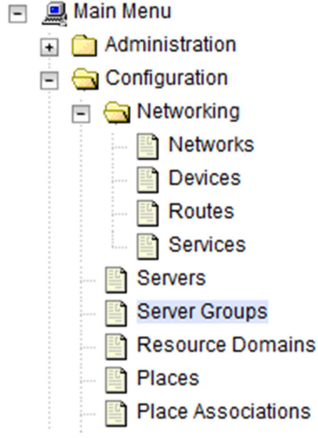

Procedure 18. Configure the SOAM Servers

7 <input type="checkbox"/>	First SOAM Server: Verify Server Health	<p>After the system reboots, login again as the admusr user.</p> <p>Execute the following command and make sure that no errors are returned:</p> <pre># 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</pre>
8 <input type="checkbox"/>	Insert and Configure the 2 nd SOAM server, repeat steps 1 through 7 for 2 nd SOAM	<p>Repeat this procedure to insert and configure the 2nd SOAM server.</p> <p>Enter the network data for the 2nd SOAM server, transfer the TKLCConfigData file to the 2nd SOAM server, and reboot the 2nd SOAM server when asked at a terminal window.</p> <p>Wait approximately 5 minutes for the 2nd SOAM server to reboot.</p> <p>Note: For DSR mated sites, repeat this step for additional/spare SOAM server for mated site.</p>


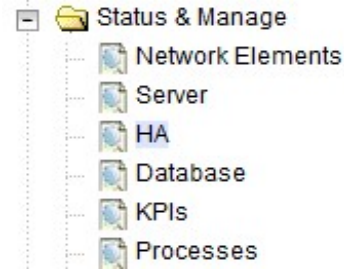
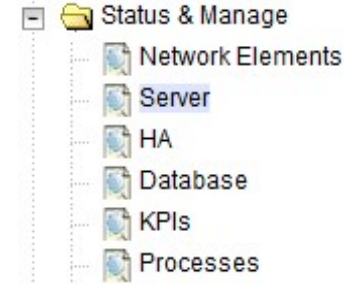
Procedure 19. Configure the SOAM Server Group

S T E P #	<p>This procedure configures the SOAM server group.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
<p>1</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Enter SOAM server group data</p> <p>From the GUI session on the NOAM VIP address, navigate to Main Menu->Configuration->Server Groups.</p>  <p>Click Insert and add the SOAM Server Group name along with the values for the following fields:</p> <div data-bbox="467 1016 854 1075"> <input type="button" value="Insert"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Report"/> </div> <p> Name: [Type Server Group Name] Level: B Parent: [Select the NOAM Server Group] Function: DSR (Active/Standby Pair) WAN Replication Connection Count: Use Default Value </p> <p>Click OK when all fields are filled.</p> <p>Note: 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.</p>

Procedure 19. Configure the SOAM Server Group

<p>2</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Edit the SOAM server group and add VIP</p>	<p>Navigate to Main Menu->Configuration->Server Groups.</p>  <p>Select the new SOAM server group and click Edit.</p> <table border="1"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>S01</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> <tr> <td>S02</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> </tbody> </table> <p>Add both SOAM servers to the server group primary site by marking the Include in SG checkbox.</p> <p>Click Apply.</p> <p>Click Add to add a SOAM VIP. Type the VIP Address and click OK:</p> 	Server	SG Inclusion	Preferred HA Role	S01	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare	S02	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
S01	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare									
S02	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare									
<p>3</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Edit the SOAM server group and add preferred spares for site redundancy (Optional)</p>	<p>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.</p> <table border="1"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>S01</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> <tr> <td>S02</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input checked="" type="checkbox"/> Prefer server as spare</td></tr> </tbody> </table> <p>For more information about server group secondary site or site redundancy, see the Terminology section.</p>	Server	SG Inclusion	Preferred HA Role	S01	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare	S02	<input checked="" type="checkbox"/> Include in SG	<input checked="" type="checkbox"/> Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
S01	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare									
S02	<input checked="" type="checkbox"/> Include in SG	<input checked="" type="checkbox"/> Prefer server as spare									

Procedure 19. Configure the SOAM Server Group

4	Primary NOAM VIP GUI: Edit the SOAM server group and add additional SOAM VIPs (Optional)	<p>Click Add to add SOAM VIPs. Type the VIP Address and click OK.</p> <p>Note: Additional SOAM VIPs only apply to SOAM server groups with preferred spare SOAMs.</p> 
5	Primary NOAM VIP GUI: Wait for replication	<p>After replication, the server status should be active (Main Menu->Status & Manage->HA).</p>  <p>Note: This may take up to 5 minutes while the servers figure out master/slave relationship.</p> <p>Look for the alarm ID 10200 Remote Database re-initialization in progress to be cleared before proceeding (Main Menu->Alarms->View Active).</p>
6	Primary NOAM VIP GUI: Restart 1 st SOAM server	<p>From the NOAM GUI, navigate to Main Menu->Status & Manage->Server and select the 1st SOAM server.</p>  <p>Click Restart. Click OK to the confirmation popup. Wait for restart to complete. Wait for the Appl State to change to Enabled, and all other columns to Norm.</p>
7	Primary NOAM VIP GUI: Restart 2 nd SOAM server	<p>Repeat step 6 for the second SOAM.</p>

Procedure 19. Configure the SOAM Server Group

8 <input type="checkbox"/>	Primary NOAM VIP GUI: Restart all preferred spare SOAM servers (Optional)	If additional preferred spare servers are configured for secondary sites, navigate to Main Menu->Status & Manage->Server and select all Preferred Spare SOAM servers. Click Restart . Click OK to the confirmation popup. Wait for the Appl State to change to Enabled and all other columns to change to Norm .
-------------------------------	---	---

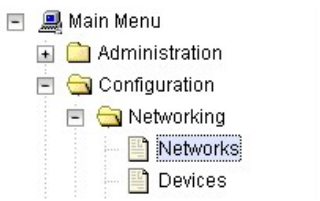


Procedure 20. Activate PCA/DCA (PCA/DCA Only)

S T E P #		This procedure activates PCA/DCA. 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 <input type="checkbox"/>	(PCA Only) Activate PCA feature	If you are installing PCA, execute the applicable procedures (added SOAM site activation or complete system activation) from [2] DSR PCA Activation Guide, E81528 to activate PCA. Note: If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online. Note: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.
2 <input type="checkbox"/>	(DCA Only) Activate DCA feature	If you are installing PCA, execute [24] DCA Framework and Application Activation and Deactivation Guide, E80801 to activate the DCA framework and feature. Note: If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online. Note: Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

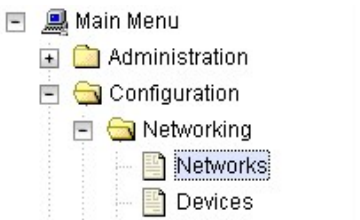

Procedure 21. Configure the MP Virtual Machines

S T E P #		This procedure configures MP VMs (IPFE, SBR, SS7-MP, DA-MP). 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 <input type="checkbox"/>	Primary NOAM VIP GUI: 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.

Procedure 21. Configure the MP Virtual Machines

<p>2</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Navigate to the signaling network configuration screen</p>	<p>Navigate to Main Menu->Configuration->Networking->Networks.</p>  <p>Navigate to the SO Network Element tab under which the MPs are to be configured.</p>  <p>Click Insert in the lower left corner.</p> 																											
<p>3</p> <p><input type="checkbox"/></p>	<p>Primary NOAM VIP GUI: Add signaling networks</p>	<p>The following screen displays:</p> <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Network Name *</td><td>XSI2</td><td>The name of this network. [Default = N/A. Range = Alphanumeric string up to 31 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 = N/A. Range = 1-4094.] [A value is required.]</td></tr> <tr> <td>Network Address *</td><td>10.196.226.0</td><td>The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon</td></tr> <tr> <td>Netmask *</td><td>255.255.255.0</td><td>Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6)</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 of the default route or enabled, this address will be the one monitored.</td></tr> <tr> <td>Default Network</td><td><input type="radio"/> Yes <input checked="" type="radio"/> No</td><td>A selection indicating whether this is the network with a default gateway.</td></tr> <tr> <td>Routed</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</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> <p>Ok Apply Cancel</p> <p>Type the Network Name, Network Type, VLAN ID, Network Address, Netmask, and Router IP that matches the signaling network.</p> <p>Note: Even if the network does not use VLAN tagging, you should type the correct VLAN ID here as indicated by the NAPD.</p> <p>Select Signaling for Network Type</p> <p>Select No for Default Network.</p> <p>Select Yes for Routable.</p> <p>Click OK if you are finished adding signaling networks</p> <p>-OR-</p> <p>Click Apply to save this signaling network and repeat this step to enter additional signaling networks.</p>	Field	Value	Description	Network Name *	XSI2	The name of this network. [Default = N/A. Range = Alphanumeric string up to 31 chars, starting with a letter.] [A value is required.]	Network Type	Signaling	The type of this network.	VLAN ID *	7	The VLAN ID to use for this network. [Default = N/A. Range = 1-4094.] [A value is required.]	Network Address *	10.196.226.0	The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon	Netmask *	255.255.255.0	Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6)	Router IP		The IP address of a router on this network. If this is a default network, this will be used as the gateway address of the default route or enabled, this address will be the one monitored.	Default Network	<input type="radio"/> Yes <input checked="" type="radio"/> No	A selection indicating whether this is the network with a default gateway.	Routed	<input checked="" type="radio"/> Yes <input type="radio"/> No	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.
Field	Value	Description																											
Network Name *	XSI2	The name of this network. [Default = N/A. Range = Alphanumeric string up to 31 chars, starting with a letter.] [A value is required.]																											
Network Type	Signaling	The type of this network.																											
VLAN ID *	7	The VLAN ID to use for this network. [Default = N/A. Range = 1-4094.] [A value is required.]																											
Network Address *	10.196.226.0	The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon																											
Netmask *	255.255.255.0	Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6)																											
Router IP		The IP address of a router on this network. If this is a default network, this will be used as the gateway address of the default route or enabled, this address will be the one monitored.																											
Default Network	<input type="radio"/> Yes <input checked="" type="radio"/> No	A selection indicating whether this is the network with a default gateway.																											
Routed	<input checked="" type="radio"/> Yes <input type="radio"/> No	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.																											

Procedure 21. Configure the MP Virtual Machines

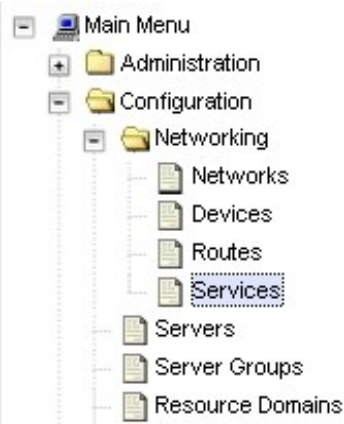
4	Primary NOAM VIP GUI: (PCA/DCA only) Navigate to signaling network configuration screen	<p>Note: Execute this step only if you are defining a separate, dedicated network for SBR Replication.</p> <p>Navigate to Main Menu->Configuration->Networking->Networks.</p>  <p>Navigate to the respective SOAM NE tab.</p> <p>Click Insert in the lower left corner.</p> 																											
5	Primary NOAM VIP GUI: (PCA only) Define SBR DB replication network	<p>Note: Execute this step only if you are defining a separate, dedicated network for SBR replication.</p> <table border="1" data-bbox="505 835 1401 1381"> <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 = N/A. Range = Alphanumeric string up to 31 chars, 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>9</td><td>The VLAN ID to use for this network. [Default = N/A. Range = 1-4094.] [A value is required.]</td></tr> <tr> <td>Network Address *</td><td>10.196.224.1</td><td>The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotted decimal notation.]</td></tr> <tr> <td>Netmask *</td><td>255.255.255.0</td><td>Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in dotted decimal notation.]</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. If enabled, this address will be the one monitored.</td></tr> <tr> <td>Default Network</td><td><input type="radio"/> Yes <input checked="" type="radio"/> No</td><td>A selection indicating whether this is the network with a default gateway.</td></tr> <tr> <td>Routed</td><td><input checked="" type="radio"/> Yes <input type="radio"/> No</td><td>Whether or not this network is routed outside its network element. If it is not assigned to a network element, it is not routed.</td></tr> </tbody> </table> <p>Ok Apply Cancel</p> <p>Type the Network Name, Network Type, VLAN ID, Network Address, Netmask, and Router IP that matches the SBR DB replication network.</p> <p>Note: Even if the network does not use VLAN tagging, you should type the correct VLAN ID here as indicated by the NAPD.</p> <p>Select No for Default Network.</p> <p>Select Yes for Routable.</p> <p>Click OK if you are finished adding signaling networks.</p> <p>-OR-</p> <p>Click Apply to save this signaling network and repeat this step to enter additional signaling networks.</p>	Field	Value	Description	Network Name *	Replication	The name of this network. [Default = N/A. Range = Alphanumeric string up to 31 chars, starting with a letter.]	Network Type	Signaling	The type of this network.	VLAN ID *	9	The VLAN ID to use for this network. [Default = N/A. Range = 1-4094.] [A value is required.]	Network Address *	10.196.224.1	The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotted decimal notation.]	Netmask *	255.255.255.0	Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in dotted decimal notation.]	Router IP		The IP address of a router on this network. If this is a default network, this will be used as the gateway address. If enabled, this address will be the one monitored.	Default Network	<input type="radio"/> Yes <input checked="" type="radio"/> No	A selection indicating whether this is the network with a default gateway.	Routed	<input checked="" type="radio"/> Yes <input type="radio"/> No	Whether or not this network is routed outside its network element. If it is not assigned to a network element, it is not routed.
Field	Value	Description																											
Network Name *	Replication	The name of this network. [Default = N/A. Range = Alphanumeric string up to 31 chars, starting with a letter.]																											
Network Type	Signaling	The type of this network.																											
VLAN ID *	9	The VLAN ID to use for this network. [Default = N/A. Range = 1-4094.] [A value is required.]																											
Network Address *	10.196.224.1	The network address of this network. [Default = N/A. Range = Valid Network Address of the network in dotted decimal notation.]																											
Netmask *	255.255.255.0	Subnetting to apply to servers within this network. [Default = N/A. Range = Valid Netmask for the network in dotted decimal notation.]																											
Router IP		The IP address of a router on this network. If this is a default network, this will be used as the gateway address. If enabled, this address will be the one monitored.																											
Default Network	<input type="radio"/> Yes <input checked="" type="radio"/> No	A selection indicating whether this is the network with a default gateway.																											
Routed	<input checked="" type="radio"/> Yes <input type="radio"/> No	Whether or not this network is routed outside its network element. If it is not assigned to a network element, it is not routed.																											
6	Primary NOAM	<p>Note: Execute this step only if you are defining a separate, dedicated</p>																											

Procedure 21. Configure the MP Virtual Machines

☐ **VIP GUI:** (PCA only) Perform additional service to networks mapping

network for SBR replication.

Navigate to **Main Menu->Configuration->Networking->Services**.



Click **Edit**.

Edit

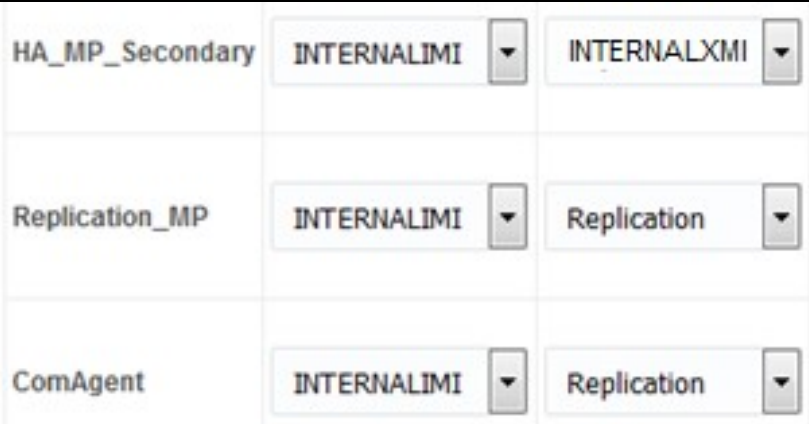
Report

Set the services using one of the following scenarios:

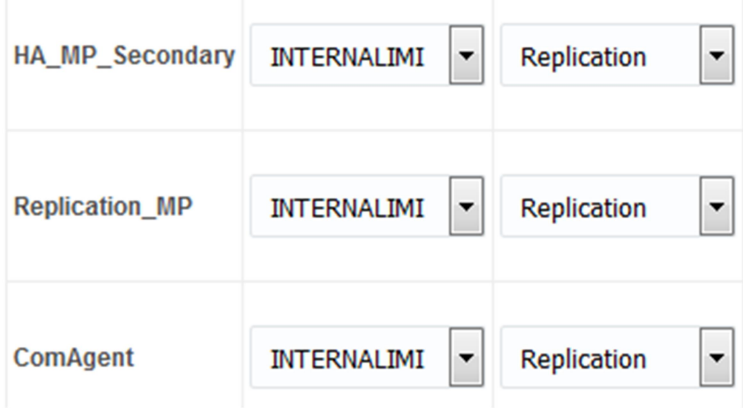
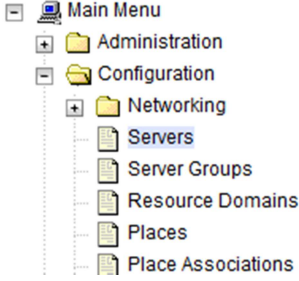
- If the dual-path HA configuration is required:**

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 database. 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>



Procedure 21. Configure the MP Virtual Machines





		<ul style="list-style-type: none"> • If the dual-path HA configuration is NOT required: <p>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.</p> <table border="1"> <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><IMI Network></td><td><SBR DB Replication Network></td></tr> <tr> <td>Replication_MP</td><td><IMI Network></td><td><SBR DB Replication Network></td></tr> <tr> <td>ComAgent</td><td><IMI Network></td><td><SBR DB Replication Network></td></tr> </tbody> </table>  <p>Click OK to apply the Service-to-Network selections.</p> 	Name	Intra-NE Network	Inter-NE Network	HA_MP_Secondary	<IMI Network>	<SBR DB Replication Network>	Replication_MP	<IMI Network>	<SBR DB Replication Network>	ComAgent	<IMI Network>	<SBR DB Replication Network>
Name	Intra-NE Network	Inter-NE Network												
HA_MP_Secondary	<IMI Network>	<SBR DB Replication Network>												
Replication_MP	<IMI Network>	<SBR DB Replication Network>												
ComAgent	<IMI Network>	<SBR DB Replication Network>												
7 <input type="checkbox"/>	Primary NOAM VIP GUI: Insert the MP or IPFE server – Part 1	<p>Navigate to Main Menu->Configuration->Servers.</p>  <p>Click Insert to add the new MP or IPFE server into servers table.</p> <div> <input type="button" value="Insert"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Export"/> <input type="button" value="Report"/> </div> <p>Fill out the following values:</p>												

Procedure 21. Configure the MP Virtual Machines

Attribute	Value
Hostname *	<input type="text"/>
Role *	- Select Role - 
System ID	<input type="text"/>
Hardware Profile	DSR Guest 
Network Element Name *	- Unassigned - 
Location	<input type="text"/>

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]

OAM Interfaces [At least one interface is required.]:		
Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	<input type="text" value="10.196.227."/>	eth0  <input type="checkbox"/> VLAN (6)
INTERNALIMI (169.254.1.0/24)	<input type="text" value="169.254.1."/>	eth0  <input type="checkbox"/> VLAN (3)
XSI-1 (10.196.228.0/25)	<input type="text" value="10.196.228."/>	eth0  <input type="checkbox"/> VLAN (26)
XSI-2 (10.196.128.0/25)	<input type="text" value="10.196.228."/>	eth0  <input type="checkbox"/> VLAN (27)

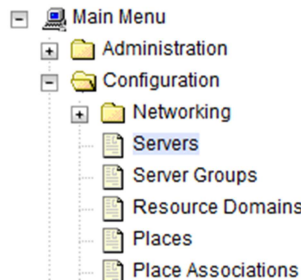
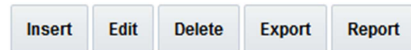
For the XMI network, type the MP's XMI IP address. Select the correct interface.

Leave the **VLAN** checkbox unmarked.

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

Leave the **VLAN** checkbox unmarked.

Procedure 21. Configure the MP Virtual Machines

		<p>For the Replication network, type the MP's XSI2 IP address. Select the correct interface. Leave the VLAN checkbox unmarked.</p> <p>For the XSI1 network, type the MP's XSI1 IP address. Select the correct interface.</p> <p>Leave the VLAN checkbox unmarked.</p> <p>For the XSI2 network, type the MP's XSI2 IP address. Select the correct interface.</p> <p>Leave the VLAN checkbox unmarked.</p> <p>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.</p> <p>Add the following NTP servers:</p> <table><tr><th>NTP Server</th><th>Preferred?</th></tr><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></table> <p>Click OK when all fields are filled in to finish MP server insertion.</p>	NTP Server	Preferred?	Valid NTP server	Yes	Valid NTP server	No	Valid NTP server	No
NTP Server	Preferred?									
Valid NTP server	Yes									
Valid NTP server	No									
Valid NTP server	No									
8 <input type="checkbox"/>	Primary NOAM VIP GUI: Export the initial configuration	<p>Navigate to Main Menu->Configuration->Servers.</p>  <p>From the GUI screen, select the MP server that was just configured and click Export to generate the initial configuration data for that server.</p>  <p>Go to the Info tab to confirm the file has been created.</p>								
9 <input type="checkbox"/>	MP Server: Log into the MP	Obtain a terminal window connection on the MP or IPFE server.								
10 <input type="checkbox"/>	Primary NOAM VIP GUI: Copy configuration file to MP or IPFE server	<p>From the active NOAM console, login as the admusr user.</p> <pre>\$ sudo scp /var/TKLC/db/filemgmt/TKLCCConfigData.<hostname>.sh admusr@<ipaddr>:/var/tmp/TKLCCConfigData.sh</pre> <p>Note: ipaddr is the XMI IP address of the MP or IPFE.</p>								

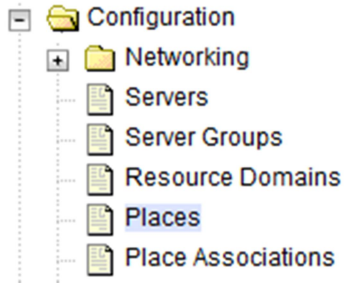
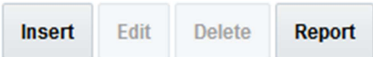
Procedure 21. Configure the MP Virtual Machines

11 <input type="checkbox"/>	MP Server: Wait for configuration to complete	<p>Obtain a terminal session on the MP or IPFE as the admusr user.</p> <p>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.</p> <p>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.</p> <p>Verify script completed successfully by checking the following file.</p> <pre>\$ sudo cat /var/TKLC/appw/logs/Process/install.log</pre> <p>Note: Ignore the warning about removing the USB key since no USB key is present.</p>
12 <input type="checkbox"/>	MP Server: Reboot the server	<p>Obtain a terminal session on the MP or IPFE as the admusr user.</p> <pre>\$ sudo init 6</pre> <p>Wait for server to reboot.</p>
14 <input type="checkbox"/>	MP Server: Verify server health	<p>After the reboot, login as the admusr user.</p> <p>Execute the following command as super-user on the server and make sure that no errors are returned:</p> <pre>\$ sudo syscheck</pre> <pre>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</pre>
15 <input type="checkbox"/>	MP Server: Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network (Optional)	<p>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.</p> <p>Log into the MP as the admusr user. (Alternatively, you can log into the VM's console.)</p> <p>Determine <XMI_Gateway_IP> from your SO site network element info.</p> <p>Gather the following items:</p> <pre><NO_XMI_Network_Address> <NO_XMI_Network_Netmask></pre> <p>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.</p> <p>[MP console] Create network routes to the NO's XMI(OAM) network:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=net</pre>

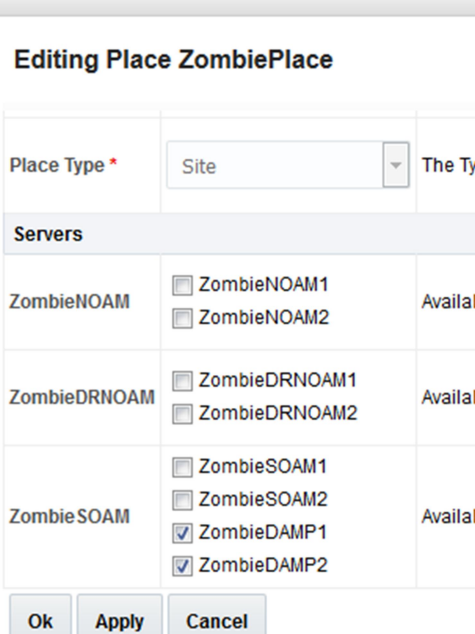
Procedure 21. Configure the MP Virtual Machines

		<pre>--address=<NO_Site_Network_ID> --netmask=<NO_Site_Network_Netmask> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface></pre> <p>Route to <MP_XMI_Interface> added.</p> <p>(Optional) [MP console] If sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm add --route=host --address=<Customer_NMS_IP> --gateway=<MP_XMI_Gateway_IP_Address> --device=<MP_XMI_Interface></pre> <p>Route to <MP_XMI_Interface> added.</p> <p>Repeat for any existing customer NMS stations.</p> <p>Delete the existing default route:</p> <pre>\$ sudo /usr/TKLC/plat/bin/netAdm delete -- route=default --gateway=<MP_XMI_Gateway_IP> -- device=<MP_XMI_Interface></pre> <p>Route to <MP_XMI_Interface> removed.</p> <p>[MP Console] Ping active NO XMI IP address to verify connectivity:</p> <pre>\$ ping <ACTIVE_NO_XMI_IP_Address></pre> <pre>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</pre> <p>(Optional) [MP Console] Ping Customer NMS Station(s):</p> <pre>\$ ping <Customer_NMS_IP></pre> <pre>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</pre> <p>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.</p>
16 <input type="checkbox"/>	Repeat for remaining MPs and IPFEs	Repeat steps 7 through 15 for all remaining MP (SBR, SS7-MP, DA-MP, and IPFE) servers.

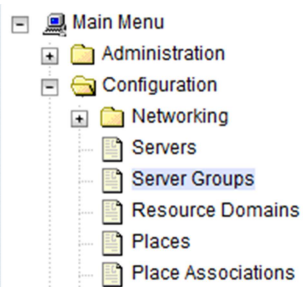
Procedure 22. Configure Places and Assign MP Servers to Places (PCA and DCA Only)

S T E P #	<p>This procedure adds places in the PCA network.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>																
1 <input type="checkbox"/>	(PCA Only) Primary NOAM VIP GUI: Configure Places	<p>Establish a GUI session on the NOAM by using the XMI VIP address. Login as the guiadmin user.</p> <p>Navigate to Main Menu->Configuration->Places.</p>  <p>Click Insert.</p>  <p>Inserting a new Place</p> <table border="1" data-bbox="506 1024 1315 1411"> <thead> <tr> <th colspan="3">Place</th></tr> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Place Name *</td><td><input type="text" value="ZombiePlace"/></td><td>Unique identifier used to label a Place. [Default and space.] [A value is required.]</td></tr> <tr> <td>Parent *</td><td><input type="text" value="NONE"/></td><td>The Parent of this Place [A value is required.]</td></tr> <tr> <td>Place Type *</td><td><input type="text" value="Site"/></td><td>The Type of this Place [A value is required.]</td></tr> </tbody> </table> <p>Place Name: <Site Name> Parent: NONE Place Type: Site</p> <p>Repeat this step for each of the PCA/DCA Places (Sites) in the network.</p> <p>See the Terminology section for more information on Sites & Places.</p>	Place			Field	Value	Description	Place Name *	<input type="text" value="ZombiePlace"/>	Unique identifier used to label a Place. [Default and space.] [A value is required.]	Parent *	<input type="text" value="NONE"/>	The Parent of this Place [A value is required.]	Place Type *	<input type="text" value="Site"/>	The Type of this Place [A value is required.]
Place																	
Field	Value	Description															
Place Name *	<input type="text" value="ZombiePlace"/>	Unique identifier used to label a Place. [Default and space.] [A value is required.]															
Parent *	<input type="text" value="NONE"/>	The Parent of this Place [A value is required.]															
Place Type *	<input type="text" value="Site"/>	The Type of this Place [A value is required.]															

Procedure 22. Configure Places and Assign MP Servers to Places (PCA and DCA Only)

2	NOAM VIP GUI: Assign MP server to places	<p>Select the place configured in step 1 and click Edit.</p>  <p>Mark all the checkboxes for SS7-MPs and PCA/DCA DA-MP and SBR servers that are assigned to this place.</p> <p>Repeat this step for all other DA-MP or SBR servers you wish to assign to places.</p> <p>Note: All DA-MPs and SBR servers must be added to the Site Place that corresponds to the physical location of the server.</p> <p>See the Terminology section for more information on Sites & Places.</p>
---	--	--

Procedure 23. Configure the MP Server Group(s) and Profiles

STEP #	<p>This procedure configures MP server groups.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1	Primary NOAM VIP GUI: Enter MP or IPFE Server Group Data	<p>From the GUI session on the NOAM VIP address, navigate to Main Menu->Configuration->Server Groups.</p>  <p>Click Insert and fill out the following fields:</p>

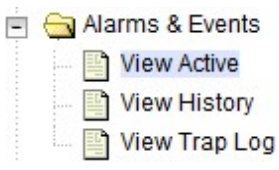
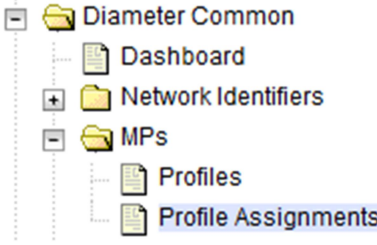
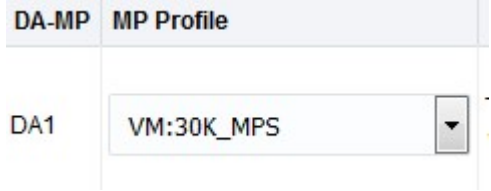
Procedure 23. Configure the MP Server Group(s) and Profiles

		Server Group Name: [Type 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 border="1"> <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>Session Binding Repository</td> <td>Session Binding Repository Function</td> <td>1 Active MP and 1 Standby MP/Per SG</td> </tr> <tr> <td>IP Front End</td> <td>IPFE application</td> <td>Multiple MPs active per SG. Each TSA may be hosted by any one of the IPFEs.</td> </tr> <tr> <td>Policy & Charging SBR</td> <td>Policy and Charging Session/or Policy Binding Function</td> <td>1Active MP, 1 Standby MP, 1 Optional Spare Per SG</td> </tr> <tr> <td>SS7-IWF</td> <td>MAP IWF Application</td> <td>1 Active MP per SG</td> </tr> </tbody> </table> <p>For PCA application:</p> <ul style="list-style-type: none"> • Online Charging function(only) <p>At least one MP Server Group with the Policy and Charging SBR function must be configured.</p> <p>At least one MP Server Group with the DSR (multi-active cluster) function must be configured.</p> <ul style="list-style-type: none"> • Policy DRA function <p>At least two MP Server Groups with the Policy and Charging SBR function must be configured. One stores session data and one stores binding data.</p> <p>At least one MP Server Group with the DSR (multi-active cluster) function must be configured</p> <p>WAN Replication Connection Count:</p> <p>For non-Policy and Charging SBR Server Groups: Default Value For Policy and Charging Server Groups: 8</p> <p>For the PCA application, the following types of MP Server Groups must be configured:</p> <p>DA-MP (Function: DSR (multi-active cluster)) SBR (Function: Policy and Charging SBR) IPFE (Function: IP Front End)</p> <p>Click OK when all fields are filled in.</p>	Server Group Function	MPs Will Run	Redundancy Model	DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs Active per SG	DSR (active-standby pair)	Diameter Relay and Application Services	1 Active MP and 1 Standby MP/Per SG	Session Binding Repository	Session Binding Repository Function	1 Active MP and 1 Standby MP/Per SG	IP Front End	IPFE application	Multiple MPs active per SG. Each TSA may be hosted by any one of the IPFEs.	Policy & Charging SBR	Policy and Charging Session/or Policy Binding Function	1Active MP, 1 Standby MP, 1 Optional Spare Per SG	SS7-IWF	MAP IWF Application	1 Active MP per SG
Server Group Function	MPs Will Run	Redundancy Model																					
DSR (multi-active cluster)	Diameter Relay and Application Services	Multiple MPs Active per SG																					
DSR (active-standby pair)	Diameter Relay and Application Services	1 Active MP and 1 Standby MP/Per SG																					
Session Binding Repository	Session Binding Repository Function	1 Active MP and 1 Standby MP/Per SG																					
IP Front End	IPFE application	Multiple MPs active per SG. Each TSA may be hosted by any one of the IPFEs.																					
Policy & Charging SBR	Policy and Charging Session/or Policy Binding Function	1Active MP, 1 Standby MP, 1 Optional Spare Per SG																					
SS7-IWF	MAP IWF Application	1 Active MP per SG																					

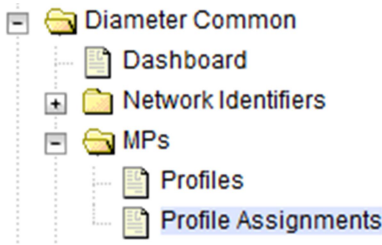
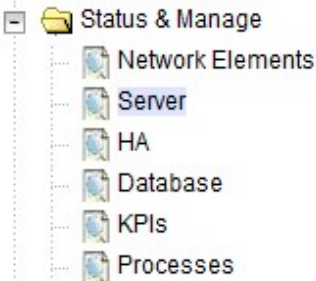
Procedure 23. Configure the MP Server Group(s) and Profiles

2 <input type="checkbox"/>	Primary NOAM VIP GUI: Repeat for additional server groups	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.									
3 <input type="checkbox"/>	Primary NOAM VIP GUI: Edit the MP server groups to include MPs	<p>Navigate to Main Menu->Configuration->Server Groups, select a server group that you just created, and click Edit.</p> <p>Select the network element representing the MP server group you wish to edit.</p> <p>Mark the Include in SG checkbox for every MP server you wish to include in this server group. Leave other checkboxes blank.</p> <table border="1"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>DAMP1</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> <tr> <td>DAMP2</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input type="checkbox"/> Prefer server as spare</td></tr> </tbody> </table> <p>Note: Each IPFE and SS7-MP server should be in its own server group.</p> <p>Click OK.</p>	Server	SG Inclusion	Preferred HA Role	DAMP1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare	DAMP2	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare
Server	SG Inclusion	Preferred HA Role									
DAMP1	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare									
DAMP2	<input checked="" type="checkbox"/> Include in SG	<input type="checkbox"/> Prefer server as spare									
4 <input type="checkbox"/>	(PCA only) Primary NOAM VIP GUI: Edit the MP server group and add preferred spares for site redundancy (Optional)	<p>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.</p> <table border="1"> <thead> <tr> <th>Server</th><th>SG Inclusion</th><th>Preferred HA Role</th></tr> </thead> <tbody> <tr> <td>SBR1</td><td><input checked="" type="checkbox"/> Include in SG</td><td><input checked="" type="checkbox"/> Prefer server as spare</td></tr> </tbody> </table> <p>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.</p> <p>Note: The preferred spare servers should be different sites from the original server. There should be servers from three separate sites (locations).</p> <p>Note: There must first be non-preferred spare present in the server group before adding the preferred spare.</p> <p>For more information about site redundancy for Policy and Charging SBR Server Groups, see the Terminology section.</p> <p>Click OK to save.</p>	Server	SG Inclusion	Preferred HA Role	SBR1	<input checked="" type="checkbox"/> Include in SG	<input checked="" type="checkbox"/> Prefer server as spare			
Server	SG Inclusion	Preferred HA Role									
SBR1	<input checked="" type="checkbox"/> Include in SG	<input checked="" type="checkbox"/> Prefer server as spare									
5 <input type="checkbox"/>	Primary NOAM VIP GUI: Repeat For additional server groups	Repeat steps 1 - 4 for any remaining MP and IPFE server groups you need to create.									

Procedure 23. Configure the MP Server Group(s) and Profiles


6	Primary NOAM VIP GUI: Wait for replication to complete on all MPs	<p>Wait for the alarm 10200: Remote Database re-initialization in progress to be cleared (Main Menu->Alarms & Events->View Active).</p>  <p>This should happen shortly after you have verified the Norm DB status in the previous step.</p>
7	SOAM VIP GUI: Assign profiles to DA-MPs from SOAM GUI	<p>Log into the GUI of the active SOAM server as the guiadmin user.</p> <p>From the SO GUI, navigate to Main Menu->Diameter Common->MPs->Profiles Assignments.</p>  <p>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.</p>  <p>For each MP, select the proper profile assignment based on the MP's type and the function it serves:</p> <ul style="list-style-type: none"> 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 <p>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.</p> <p>When finished, click Assign.</p>

Procedure 23. Configure the MP Server Group(s) and Profiles

8	<div><div></div><div>SOAM VIP GUI: Assign Profiles to SS7-MPs from SOAM GUI</div></div>	<div><div>Log into the GUI of the active SOAM server as the guiadmin user</div><div>From the SO GUI, navigate to Main Menu->Diameter->Configuration->MPs->Profiles Assignments.</div><div></div><div>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.</div><div><table><tr><th>SS7-MP</th><th>MP Profile</th><th>current value</th></tr><tr><td>SS7MP2</td><td>VM:MD-IWF</td><td>The current MP Profile for SS7MP2 is VM:MD-IWF. <i>Virtualized SS7-MP running MD-IWF application [A value is required.]</i></td></tr></table></div><div>For each SS7 MP, select the proper profile assignment based on the SS7 MP's type and the function it serves:</div><div><table><tr><th>Profile Name</th><th>Description</th></tr><tr><td>VM:MD-IWF</td><td>VM Running MAP-IWF functions</td></tr></table></div><div>When finished, click Assign.</div></div>	SS7-MP	MP Profile	current value	SS7MP2	VM:MD-IWF	The current MP Profile for SS7MP2 is VM:MD-IWF . <i>Virtualized SS7-MP running MD-IWF application [A value is required.]</i>	Profile Name	Description	VM:MD-IWF	VM Running MAP-IWF functions
SS7-MP	MP Profile	current value										
SS7MP2	VM:MD-IWF	The current MP Profile for SS7MP2 is VM:MD-IWF . <i>Virtualized SS7-MP running MD-IWF application [A value is required.]</i>										
Profile Name	Description											
VM:MD-IWF	VM Running MAP-IWF functions											
10	<div><div></div><div>Primary NOAM VIP GUI: Restart MP VM</div></div>	<div><div>From the NOAM GUI, navigate to Main Menu->Status & Manage->Server.</div><div></div><div>For each MP server:</div><div><ul style="list-style-type: none">• Select the MP server.• Click Restart.• Click OK on the confirmation screen. Wait for the message that tells you that the restart was successful.</div><div>Policy and Charging DRA/DCA Installations: You may continue to see alarms related to ComAgent until you complete PCA/DCA installation.</div></div>										

4.5. Configure Signaling Network Routes

Procedure 24. Configure the Signaling Network Routes

S T E P #	<p>This procedure configures signaling network routes on MP-type servers (DA-MP, IPFE, SBR, SS7-MP, etc.).</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<p>Establish GUI session on the NOAM VIP</p> <p>Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the guiadmin user.</p>  <p>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</p> <p>Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</p>

Procedure 24. Configure the Signaling Network Routes

2	<div><div></div><div>NOAM VIP: Navigate to routes configuration screen</div></div>	<div><div><div><div><div></div><div>Configuration</div></div><div><div></div><div>Networking</div></div><div><div></div><div>Networks</div></div><div><div></div><div>Devices</div></div><div><div></div><div>Routes</div></div><div><div></div><div>Services</div></div></div></div><div>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.</div><div><div><div>Entire Network</div><div>DA_SG</div><div>IPFE1_SG</div><div>IPFE2_SG</div><div>NO_SG</div><div>SBRb_SG</div><div>SBRs_SG</div><div>SO_SG</div><div>SS7_SG</div></div><div><div>NO1</div><div>NO2</div><div>SO1</div><div>DAMP1</div><div>DAMP2</div><div>IPFE1</div><div>IPFE2</div><div>SS7MP1</div><div>SBR-b</div><div>SBR-s</div><div>SS7MP2</div></div><table><thead><tr><th>Route Type</th><th>Destination</th><th>Netmask</th><th>Gateway</th><th>Device Name</th><th>Route Scope</th><th>Configuration Status</th><th>Is Locked?</th></tr></thead><tbody><tr><td>default</td><td>0.0.0.0</td><td></td><td>10.196.227.1</td><td>eth0</td><td>Server</td><td>Discovered</td><td>Locked</td></tr></tbody></table></div></div>	Route Type	Destination	Netmask	Gateway	Device Name	Route Scope	Configuration Status	Is Locked?	default	0.0.0.0		10.196.227.1	eth0	Server	Discovered	Locked
Route Type	Destination	Netmask	Gateway	Device Name	Route Scope	Configuration Status	Is Locked?											
default	0.0.0.0		10.196.227.1	eth0	Server	Discovered	Locked											
3	<div><div></div><div>NOAM VIP: Add route</div></div>	<div><div>Click Insert at the bottom of the screen to add additional routes.</div><div><div>Insert</div><div>Edit</div><div>Delete</div><div>Report</div><div>Report All</div></div></div>																
4	<div><div></div><div>Primary NOAM VIP GUI: Add default route for MPs going through signaling network gateway (Optional)</div></div>	<div><div>***OPTIONAL — Only execute this step if you performed MP Server: Delete Auto-Configured Default Route on MP and Replace it with a Network Route via the XMI Network (Optional), which removed the XMI gateway default route on MPs.***</div><div>To delete the default route:</div><div><div>1. Log into the primary NOAM VIP GUI.</div><div>2. Navigate to Configuration->Networking->Networks.</div><div>3. Select the specific SO tab.</div><div>4. Select the XMI network and click Unlock.</div><div>5. Click OK to confirm.</div><div>6. Navigate to Configuration->Networking->Routes.</div><div>7. Select the specific MP XMI route and click Delete.</div><div>8. Click OK to confirm.</div><div>9. Repeat steps 1 through 8 for all required MPs to delete the XMI routes.</div><div>10. Navigate to Configuration->Networking->Networks.</div><div>11. Select the specific SO tab.</div><div>12. Select the XMI network and click Lock.</div><div>13. Click OK to confirm.</div></div><div>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.</div></div>																

Procedure 24. Configure the Signaling Network Routes

Insert Route on DAMP1		
Field	Value	Description
Route Type *	<input type="radio"/> Net <input checked="" type="radio"/> Default <input type="radio"/> Host	Select a route type. [Default = N/A. Options = Net,
Device *	eth3 ▼	Select the network device name through which tra [A value is required.]
Destination		The destination network address. [Default = N/A. F
Netmask		A valid netmask for the network route destination I
Gateway IP *		The IP address of the gateway for this route. [Def:
<div> <input type="button" value="Ok"/> <input type="button" value="Apply"/> <input type="button" value="Cancel"/> </div>		
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.		
Click OK .		

Procedure 24. Configure the Signaling Network Routes

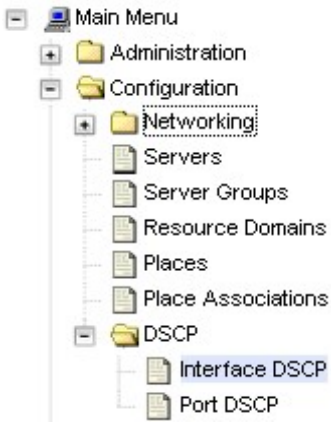
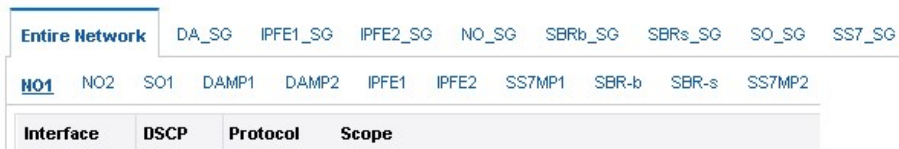

5	Primary NOAM VIP GUI: Add network routes for Diameter peers	<p>Use this step to add IP4 and/or IPv6 routes to Diameter peer destination networks. The goal here is to ensure that Diameter traffic uses the gateway(s) on the signaling networks.</p> <p>Insert Route on BuenosAires-DAMP1</p> <table border="1"> <thead> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Route Type</td><td> <input checked="" type="radio"/> Net <input type="radio"/> Default <input type="radio"/> Host * </td><td>Select a route type. [Default = N/A. Options = Net, Default, Host. You can configure at most one IPV4 default route and one IPV6 default route on a given target machine.]</td></tr> <tr> <td>Device</td><td>eth2 *</td><td>Select the network device name through which traffic is being routed. The selection of AUTO will result in the device being selected automatically, if possible. [Default = N/A. Range = Provisioned devices on the selected server.]</td></tr> <tr> <td>Destination</td><td></td><td>The destination network address. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon hex (IPv6) format.]</td></tr> <tr> <td>Netmask</td><td></td><td>A valid netmask for the network route destination IP address. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6) or dotted decimal (IPv4) format.]</td></tr> <tr> <td>Gateway IP</td><td></td><td>The IP address of the gateway for this route. [Default = N/A. Range = Valid IP address of the gateway in dotted decimal (IPv4) or colon hex (IPv6) format.]</td></tr> </tbody> </table> <p>Ok Apply Cancel</p> <p>Route Type: Net</p> <p>Device: Select the appropriate signaling interface that is used to connect to that network</p> <p>Destination: Type the Network ID of network to which the peer node is connected to</p> <p>Netmask: Type the corresponding Netmask</p> <p>Gateway IP: Type the IP of the customer gateway.</p> <p>If you have more routes to enter, click Apply to save the current route entry. Repeat this step to enter more routes.</p> <p>If you have finished entering routes, click OK to save the latest route and leave this screen.</p>	Field	Value	Description	Route Type	<input checked="" type="radio"/> Net <input type="radio"/> Default <input type="radio"/> Host *	Select a route type. [Default = N/A. Options = Net, Default, Host. You can configure at most one IPV4 default route and one IPV6 default route on a given target machine.]	Device	eth2 *	Select the network device name through which traffic is being routed. The selection of AUTO will result in the device being selected automatically, if possible. [Default = N/A. Range = Provisioned devices on the selected server.]	Destination		The destination network address. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon hex (IPv6) format.]	Netmask		A valid netmask for the network route destination IP address. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6) or dotted decimal (IPv4) format.]	Gateway IP		The IP address of the gateway for this route. [Default = N/A. Range = Valid IP address of the gateway in dotted decimal (IPv4) or colon hex (IPv6) format.]
Field	Value	Description																		
Route Type	<input checked="" type="radio"/> Net <input type="radio"/> Default <input type="radio"/> Host *	Select a route type. [Default = N/A. Options = Net, Default, Host. You can configure at most one IPV4 default route and one IPV6 default route on a given target machine.]																		
Device	eth2 *	Select the network device name through which traffic is being routed. The selection of AUTO will result in the device being selected automatically, if possible. [Default = N/A. Range = Provisioned devices on the selected server.]																		
Destination		The destination network address. [Default = N/A. Range = Valid Network Address of the network in dotted decimal (IPv4) or colon hex (IPv6) format.]																		
Netmask		A valid netmask for the network route destination IP address. [Default = N/A. Range = Valid Netmask for the network in prefix length (IPv4 or IPv6) or dotted decimal (IPv4) format.]																		
Gateway IP		The IP address of the gateway for this route. [Default = N/A. Range = Valid IP address of the gateway in dotted decimal (IPv4) or colon hex (IPv6) format.]																		
6	Repeat steps 2-5 for all other MP server groups	<p>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.</p>																		

4.6. Configure DSCP (Optional)



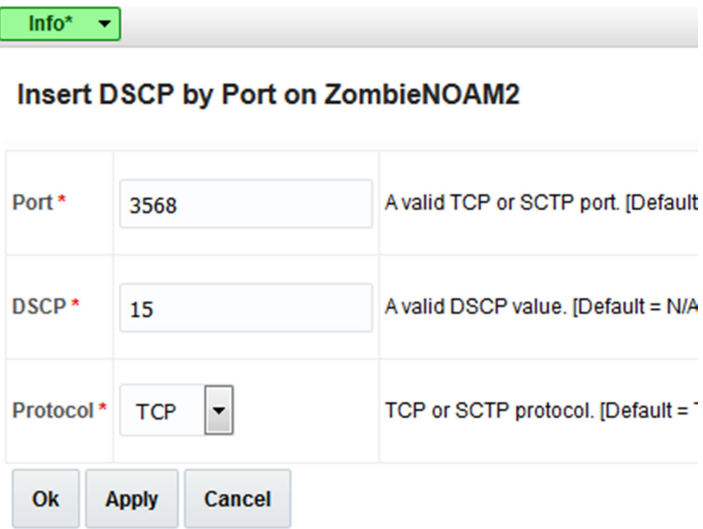
Procedure 25. Configure DSCP Values for Outgoing Traffic (Optional)

S T E P #	<p>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 has been decided that your network uses packet DSCP markings for Quality-of-Service purposes.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<div> <div> Primary NOAM VIP GUI: Establish GUI session on the NOAM VIP </div> <div> Establish a GUI session on the NOAM by using the NOAM VIP address. Login as the guiadmin user. </div> </div> <div>  </div>

Procedure 25. Configure DSCP Values for Outgoing Traffic (Optional)

2	Primary NOAM VIP GUI: Option 1: Configure interface DSCP	<p>Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary.</p> <p>Navigate to Main Menu->Configuration->Networking>DSCP->Interface DSCP.</p>  <p>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.</p> <p>Click Insert.</p>  <p>Select the network Interface from the list, and type the DSCP value to apply to packets leaving this interface.</p>  <p>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.</p>
---	---	---

Procedure 25. Configure DSCP Values for Outgoing Traffic (Optional)

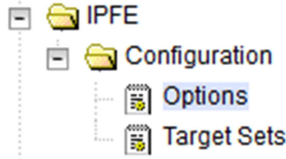
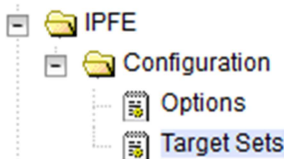
3 <input type="checkbox"/>	Primary NOAM VIP GUI: Option 2: Configure port DSCP	<p>Note: The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site will vary.</p> <p>Navigate to Main Menu->DSCP->Port DSCP.</p>  <p>Select the server to configure from 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.</p> <p>Click Insert.</p> <p>Main Menu: Configuration -> DSCP -> Port DSCP</p>  <p>Type the source Port and DSCP value, and select the transport Protocol.</p> <p>Main Menu: Configuration -> DSCP -> Port DSCP</p>  <p>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.</p>
4 <input type="checkbox"/>	Repeat for additional servers	Repeat steps 2-3 for all remaining servers.

4.7. Configure IP Front End (Optional)

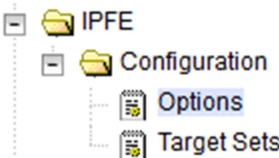
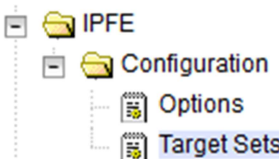
Procedure 26. IP Front End (IPFE) Configuration

STEP #	<p>This procedure configures IP Front End (IPFE) and optimizes performance.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<p>SOAM VIP: Login Log into the SOAM VIP GUI as the guiadmin user.</p> <p>Welcome to the Oracle System Login.</p> <p>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.</p> <p>Unauthorized access is prohibited.</p> <hr/> <p><i>Oracle and Java are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.</i></p> <p><i>Copyright © 2010, 2016, Oracle and/or its affiliates. All rights reserved.</i></p>

Procedure 26. IP Front End (IPFE) Configuration

<div>2</div> <div></div>	<div>SOAM VIP:</div> <div>Configuration of replication IPFE association data</div>	<div>Navigate to Main Menu->IPFE->Configuration->Options.</div> <div></div> <div>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.</div> <div>If applicable, type the address of the 3rd and 4th IPFE servers in IPFE-B1 IP Address and IPFE-B2 IP Address fields.</div> <div><table><thead><tr><th>Variable</th><th>Value</th><th>Description</th></tr></thead><tbody><tr><td colspan="3">Inter-IPFE Synchronization</td></tr><tr><td>IPFE-A1 IP Address</td><td>169.254.1.26 - 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>169.254.1.27 - 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><unset></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><unset></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></div> <div>Note: It is recommended the address reside on the IMI (Internal Management Interface) network.</div> <div>Note: IPFE-A1 and IPFE-A2 must have connectivity between each other via these addresses. The same applies with IPFE-B1 and IPFE-B2.</div>	Variable	Value	Description	Inter-IPFE Synchronization			IPFE-A1 IP Address	169.254.1.26 - IPFE1	IPv4 or IPv6 address of IPFE-A1. This selection is disabled when a Target Set has IPFE-A1 selected as Active.	IPFE-A2 IP Address	169.254.1.27 - IPFE2	IPv4 or IPv6 address of IPFE-A2. This selection is disabled when a Target Set has IPFE-A2 selected as Active.	IPFE-B1 IP Address	<unset>	IPv4 or IPv6 address of IPFE-B1. This selection is disabled when a Target Set has IPFE-B1 selected as Active.	IPFE-B2 IP Address	<unset>	IPv4 or IPv6 address of IPFE-B2. This selection is disabled when a Target Set has IPFE-B2 selected as Active.
Variable	Value	Description																		
Inter-IPFE Synchronization																				
IPFE-A1 IP Address	169.254.1.26 - IPFE1	IPv4 or IPv6 address of IPFE-A1. This selection is disabled when a Target Set has IPFE-A1 selected as Active.																		
IPFE-A2 IP Address	169.254.1.27 - IPFE2	IPv4 or IPv6 address of IPFE-A2. This selection is disabled when a Target Set has IPFE-A2 selected as Active.																		
IPFE-B1 IP Address	<unset>	IPv4 or IPv6 address of IPFE-B1. This selection is disabled when a Target Set has IPFE-B1 selected as Active.																		
IPFE-B2 IP Address	<unset>	IPv4 or IPv6 address of IPFE-B2. This selection is disabled when a Target Set has IPFE-B2 selected as Active.																		
<div>3</div> <div></div>	<div>SOAM VIP:</div> <div>Configuration of IPFE target sets (Part 1)</div>	<div>Log into the SOAM VIP GUI as the guiadmin user.</div> <div>Navigate to Main Menu->IPFE->Configuration->Target Sets.</div> <div></div> <div>Click either Insert IPv4 or Insert IPv6, depending on the IP version of the target set you plan to use.</div> <div>This screen displays the following configurable settings:</div> <div><div>Protocols:</div><div>Protocols the target set supports.</div><div><table><tr><td>Protocols</td><td><div><div>TCP only</div><div>SCTP only</div><div>Both TCP and SCTP</div></div></td></tr></table></div></div> <div><div>Delete Age:</div><div>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</div></div>	Protocols	<div><div>TCP only</div><div>SCTP only</div><div>Both TCP and SCTP</div></div>																
Protocols	<div><div>TCP only</div><div>SCTP only</div><div>Both TCP and SCTP</div></div>																			



Procedure 26. IP Front End (IPFE) Configuration

		<p>server.</p> <p>Delete Age * <input type="text" value="600"/></p> <p>Load Balance Algorithm: Hash or Least Load options.</p> <p>Load Balance Algorithm <input type="radio"/> Hash <input checked="" type="radio"/> Least Load</p> <p>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.</p>  <p>Note: The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios.</p>
4	<p>SOAM VIP:</p> <p>Configuration of IPFE target sets (Part 2)</p>	<p>Navigate to Main Menu->IPFE->Configuration->Target Sets.</p>  <p>(Optional): If you have selected the Least Load algorithm, then you may configure the following fields to adjust the algorithm's behavior:</p> <p>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.</p> <p>MPS Factor * <input type="text" value="50"/></p> <p>Connection Count Factor * <input type="text" value="50"/></p>

Procedure 26. IP Front End (IPFE) Configuration

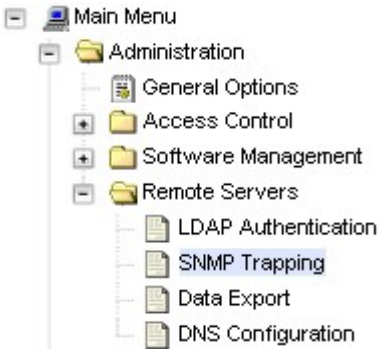
		<p>Connection Count Factor: This is the other component of the least load algorithm. This field allows you to set it from 0 (not used in load calculations) to 100 (the only component used for load calculations). Increase this setting if connection storms (the arrival of many connections at a very rapid rate) are a concern.</p> <p>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.</p> <p>Allowed Deviation * <input type="text" value="5"/></p> <p>Primary Public IP Address: IP address for the target set.</p> <div data-bbox="500 695 1057 936"> <p>Public IP Address</p> <p>Address * <input type="text"/></p> <p>Active IPFE</p> <p> <input checked="" type="radio"/> IPFE A1 ----- <input type="radio"/> IPFE A2 <input type="radio"/> IPFE B1 ----- <input type="radio"/> IPFE B2 </p> </div> <p>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).</p> <p>Active IPFE: IPFE to handle the traffic for the target set address.</p> <p>Secondary Public IP Address: If this target set supports either multi-homed SCTP or Both TCP and SCTP, provide a Secondary IP Address.</p> <div data-bbox="500 1247 1166 1623"> <p>Alternate Public IP Address†</p> <p>Alternate Address <input type="text"/></p> <p>Active IPFE for alternate address</p> <p> <input checked="" type="radio"/> IPFE A1 ----- <input type="radio"/> IPFE A2 <input type="radio"/> IPFE B1 ----- <input type="radio"/> IPFE B2 </p> </div> <p>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.</p> <p>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.</p>
--	--	---

Procedure 26. IP Front End (IPFE) Configuration

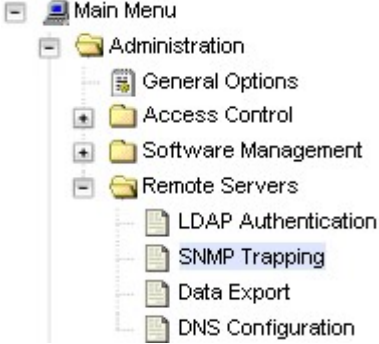
		<p>Target Set IP List: Select an IP address, a secondary IP address if supporting SCTP multi-homing, a description, and a weight for the application server.</p>  <p>Note: The IP address must be on the XSI network since they must be on the same network as the target set address. This address must also 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.</p> <p>Note: If all application servers have an equal weight (e.g., 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.</p> <p>Click Add to add more application servers (up to 16).</p> <p>Click Apply.</p> 
5	<p>SOAM VIP:</p> <p><input type="checkbox"/> Repeat for additional configuration of IPFE target sets</p>	<p>Repeat for steps 3 and 4 for each target set (up to 16).</p> <p>At least one target set must be configured.</p>

4.8. SNMP Configuration (Optional)

Procedure 27. Configure SNMP Trap Receiver(s) (Optional)

S T E P #	<p>This procedure configures forwarding of SNMP.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
<p>1</p> <p><input type="checkbox"/></p>	<p>NOAM VIP: Configure system-wide SNMP trap receiver(s)</p> <p>Using a web browser, log into the NOAM VIP as the guiadmin user. Navigate to Main Menu->Administration->SNMP.</p>  <p>Click Insert at the bottom of the screen.</p> <p>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.</p> <p>Continue to add secondary manager IPs in the corresponding fields, if needed.</p> <p>Manager 1 <input type="text"/></p> <p>Traps Enabled checkboxes can be marked on a per manager basis.</p> <p>Traps Enabled</p> <p><input type="checkbox"/> Manager 1 <input type="checkbox"/> Manager 2 <input type="checkbox"/> Manager 3 <input type="checkbox"/> Manager 4 <input type="checkbox"/> Manager 5</p> <p>Type the SNMP Community Name.</p> <p>SNMPv2c Read-Only Community Name <input type="text" value="....."/></p> <p>SNMPv2c Read-Write Community Name <input type="text"/></p> <p>Leave all other fields with their default values.</p> <p>Click OK.</p>

Procedure 27. Configure SNMP Trap Receiver(s) (Optional)

2 <input type="checkbox"/>	NOAM VIP: Enable traps from individual servers (Optional)	<p>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.</p> <p>This procedure requires all servers, including MPs, have an XMI interface on which the customer SNMP Target server (NMS) is reachable.</p> <p>Using a web browser, log into the NOAM VIP as the guiadmin user. Navigate to Main Menu->Administration->SNMP.</p>  <p>Make sure the Enabled checkbox is marked, if not, mark it as shown below:</p> <p>Traps from Individual Servers <input checked="" type="checkbox"/> Enabled</p> <p>Click Apply and verify the data is committed.</p>
-------------------------------	---	---

4.9. Create iDIH Virtual Machines (VMware)**Procedure 28. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)**

STEP #	This procedure creates the iDIH Oracle, Mediation, and Application guest.	<p>Needed material: iDIH Oracle OVA, iDIH Mediation OVA, and iDIH Application OVA.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	Add the iDIH Oracle OVA to VMware	<ol style="list-style-type: none"> 1. Launch the VMware client of your choice. 2. Add the iDIH Oracle OVA image to the VMware catalog or repository. Follow the instructions provided by the Cloud solutions manufacturer.
2 <input type="checkbox"/>	Create the Oracle VM from the OVA image	<ol style="list-style-type: none"> 1. Browse the library or repository that you placed the iDIH Oracle OVA image. 2. Deploy the OVA Image using vSphere Client or the vSphere Web Client. 3. Name the iDIH Oracle VM and select the data store.

Procedure 28. (VMware only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

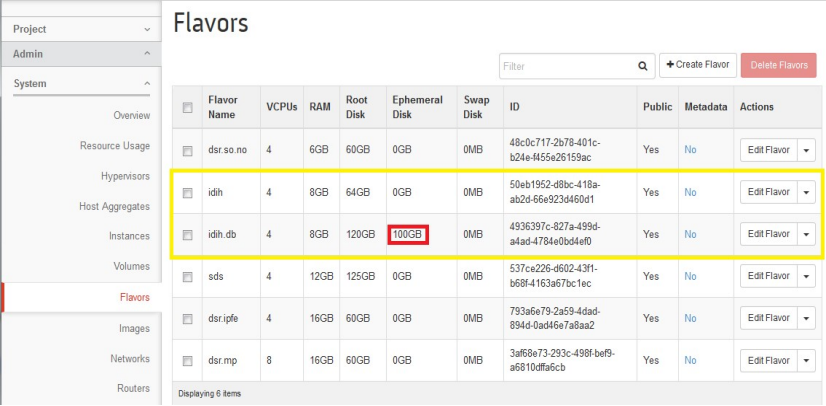
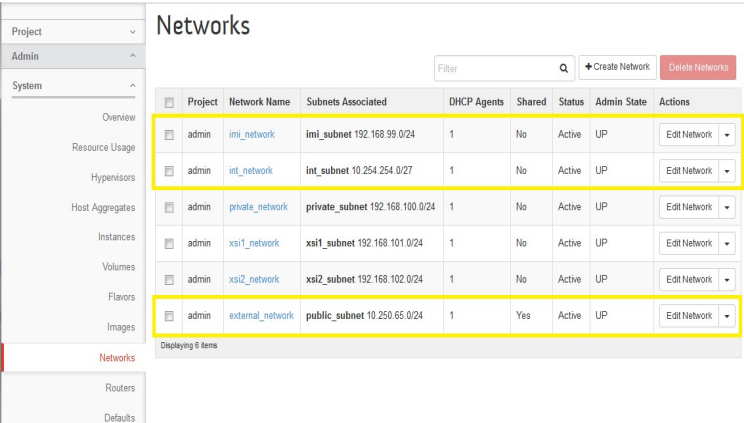
3 <input type="checkbox"/>	Configure resources for the iDIH Oracle VM	<ol style="list-style-type: none"> 1. Configure the iDIH Oracle VM per the Resource Profile in Appendix C Resource Profile for the iDIH Oracle VM using the vSphere client or the vSphere web client. 2. Record the Ethernet addresses associated with each interface and the virtual network with which it is associated. <p>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.</p>
4 <input type="checkbox"/>	iDIH Oracle VM Only: Create a raw storage block device (external device)	<p>Note: This step is ONLY required for iDIH Oracle VM.</p> <p>Create an extra disk for the Oracle VM. Add the second disk using the vSphere client or the vSphere web client.</p>
5 <input type="checkbox"/>	Power on the iDIH Oracle VM	Use the vSphere client or vSphere web client to power on the iDIH Oracle VM .
6 <input type="checkbox"/>	iDIH Oracle VM Only: Verify the extra/second disk exists	<p>Note: This step is ONLY required for iDIH Oracle VM.</p> <p>Check if the raw storage block device (external disk) added in step 3 exists by executing any of these commands:</p> <pre>\$ ls /dev/[sv]db \$ fdisk -l \$ df -h</pre> <p>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.</p>
7 <input type="checkbox"/>	Procedure Overview	<p>Repeat Steps 1 through 6 for the following VMs. Use unique labels for the VM names:</p> <p>iDIH Application iDIH Mediation</p>

4.10. Create iDIH Virtual Machines (KVM/OpenStack)

Procedure 29. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

S T E P #	<p>This procedure creates the iDIH Oracle, Mediation, and Application guest.</p> <p>Needed material: iDIH Oracle OVA, iDIH Mediation OVA, and iDIH Application OVA</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<div> <div>Add the iDIH Oracle OVA to KVM/OpenStack</div> <div> <ol style="list-style-type: none"> Copy the OVA file to the OpenStack control node. <pre>\$ scp oracle-8.0.x.x.x.ova admusr@node:~</pre> Log into the OpenStack control node. <pre>\$ ssh admusr@node</pre> In an empty directory, unpack the OVA file using tar. <pre>\$ tar xvf oracle-8.0.x.x.x.ova</pre> One of the unpacked files has a .vmdk suffix. This is the VM image file that must be imported. oracle-8.0.x.x.x-disk1.vmdk Note: The OVA format only supports files with a max size of 8GB, so a vmdk file larger than that is split. You should be able to concatenate the files together to merge them back into one file: <pre>\$ cat ORA-80_x_x.vmdk.000000000 ORA-80_x_x.vmdk.000000001 > ORA-80_x_x.vmdk</pre> Source the OpenStack admin user credentials. <pre>\$. keystone_admin</pre> Select an informative name for the new image. ORA-8.0_x_x Import the image using the glance utility from the command line. <pre>\$ glance image-create --name oracle-8.0.x.x.x-original --visibility public --protected false --progress --container-format bare --disk-format vmdk --file oracle-8.0.x.x.x-disk1.vmdk</pre> <p>This process takes about 5 minutes, depending on the underlying infrastructure.</p> </div> </div>

Procedure 29. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

<div>2</div> <div></div>	<p>Create flavors for iDIH</p>	<p>Examine the storage recommendations in the Resource Profile in Appendix C. 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.</p>  <p>The screenshot shows the 'Flavors' page in the OpenStack dashboard. A table lists several flavors: dsr.so.no, idih, idih.db, sds, dsr.igf, and dsr.mp. The 'idih.db' flavor is highlighted with a yellow box. Its specifications are: 4 VCPUs, 8GB RAM, 120GB Root Disk, 100GB Ephemeral Disk, and 0MB Swap Disk. The '100GB' value is also highlighted with a red box.</p>
<div>3</div> <div></div>	<p>Create network interfaces</p>	<p>Examine the network interface recommendations at the bottom of the Resource Profile in Appendix C. Network ports must be created for each recommended interface. For example:</p>  <p>The screenshot shows the 'Networks' page in the OpenStack dashboard. A table lists several networks: im_network, int_network, private_network, xsi1_network, xsi2_network, and external_network. The 'int_network' and 'external_network' rows are highlighted with yellow boxes. The 'int_network' has a subnet of 10.254.254.0/27, and the 'external_network' has a subnet of 10.250.65.0/24.</p>
<div>4</div> <div></div>	<p>Create and boot the iDIH VM instance from the glance image</p>	<ol style="list-style-type: none"> Get the following configuration values. <ul style="list-style-type: none"> The image ID. <pre>\$ glance image-list</pre> The flavor ID. <pre>\$ nova flavor-list</pre> The network ID(s) <pre>\$ neutron net-list</pre> An informative name for the instance. <ul style="list-style-type: none"> iDIH-Oracle iDIH-Mediation iDIH-Application Create and boot the VM instance. <p>The instance must be owned by the DSR tenant user, not the admin user.</p>

Procedure 29. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

		<p>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 interface-to-network mappings described at the bottom of the Resource Profile in Appendix C.</p> <p>Note: IPv6 addresses should use the v6-fixed-ip argument instead of v4-fixed-ip.</p> <p>For Oracle VM Only</p> <p>Create the ephemeral storage for only the Oracle VM.</p> <pre>\$ 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></pre> <p>For example:</p> <pre>\$ 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</pre> <p>For Application VM Only</p> <pre>\$ 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></pre> <p>For example:</p> <pre>\$ 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-App</pre> <p>For Mediation VM Only</p> <p>For Mediation, add the IMI interface as the IMI interface.</p> <pre>\$ 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></pre> <p>For example:</p> <pre>\$ 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 net-id=674b8461-ffed-4818-8dea-7544f9c06e5f,v4-fixed-ip=10.254.254.3 --nic net-id=3d9b9da8-96ad-4f29-9f82-98b00ea30446,v4-fixed-ip=192.168.99.3 -config-drive</pre>
--	--	--

Procedure 29. (KVM/OpenStack Only) Create iDIH Oracle, Mediation, and Application VMs (Optional)

		<pre>true iDIH-Mediation</pre> <p>3. View the newly created instance using the nova tool.</p> <pre>\$ nova list --all-tenants</pre> <p>The VM takes approximately 5 minutes to boot and may be accessed through both network interfaces and the Horizon console tool.</p>
5 <input type="checkbox"/>	Verify configured interface	<p>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:</p> <pre>\$ ping <XMI-IP-Provided-During-Nova-Boot></pre> <p>If successfully pinging, ignore the step 6 to manually configuring the interface.</p>
6 <input type="checkbox"/>	Manually configure interface, if not already done (Optional)	<p>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.</p> <ol style="list-style-type: none"> 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 to the interface-to-network mappings described at the bottom of the Resource Profile in Appendix C. <pre>\$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask></pre> <pre>\$ sudo netAdm add --onboot=yes --device=eth1 --address=<imi ip> --netmask=<imi net mask></pre> <pre>\$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip></pre> <p>Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.</p> <ol style="list-style-type: none"> 7. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting. <pre>\$ sudo init 6</pre> <p>The new VM should now be accessible via both network and Horizon consoles.</p>
7 <input type="checkbox"/>	Procedure Overview	<p>Repeat steps 1 through 4 for the following VMs. Use unique labels for the VM names:</p> <p>iDIH-Application iDIH-Mediation</p>

4.11. Create iDIH Virtual Machines - OVM-S/OVM-M (Optional)

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

S T E P #	<p>This procedure imports an iDIH image and creates and configures a VM.</p> <p>Repeat this procedure three times for:</p> <ul style="list-style-type: none"> • iDIH Oracle (db) • iDIH Application (app) • iDIH Mediation (med) <p>Replace xxx in variable names with the different suffix, when repeating.</p> <p>This procedure requires values for these variables:</p> <p><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 XMI> <OVM network ID for IDIH Internal> <OVM network ID for IMI></p> <p>Execution of this procedure discovers and uses the values of these variables:</p> <p><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#></p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
----------------------------------	---

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

<div data-bbox="178 264 237 333" data-label="Text">1</div> <div data-bbox="178 333 237 1012" data-label="Image"> </div>	<div data-bbox="237 264 466 1012" data-label="Text">Preparation</div>	<div data-bbox="466 264 1429 583" data-label="Text"> <p>Refer to Appendix E Common OVM-Manager Tasks (CLI) to set up the platform.</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <OVM-M IP>. <OVM-M IP> = 100.64.62.122 2. Copy and paste the value for <OVM-M IP> into the command. <pre>ssh -l admin <OVM-M IP> -p 1000</pre> For example, <code>ssh -l admin 100.64.62.221 -p 1000</code> 3. Alternatively, use a terminal emulation tool like PUTTY. </div> <div data-bbox="466 583 1429 1012" data-label="Image"> </div>
---	---	--

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

2	OVM-M CLI: <input type="checkbox"/> Import the OVA for iDIH	<p>Import the Virtual Appliance/OVA for iDIH-xxx.</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <MyRepository name> and <URL to iDIH-xxx>. <p><MyRepository name> = XLab Utility Repo01</p> <p><URL to iDIH-xxx> = http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova</p> <ol style="list-style-type: none"> 2. Copy and paste the values for <MyRepository name> and <URL to iDIH-xxx> into the command. <pre>OVM>importVirtualAppliance Repository name='<MyRepository Name>' url=<URL to IDIH-XXX OVA></pre> <p>Example:</p> <pre>OVM>importVirtualAppliance Repository name='XLab Utility Repo01' url=http://10.240.155.70/iso/IDIH/8.0/ova/oracle- 8.0.0.0.0_80.19.1.1.ova</pre> <ol style="list-style-type: none"> 3. Execute the command and validate success. 4. From the screen results, find the site specific text (highlighted). <p>Command: importVirtualAppliance Repository name='XLab Utility Repo01'</p> <p>url=http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova</p> <p>Status: Success</p> <p>Time: 2017-04-18 15:23:31,044 EDT</p> <p>JobId: 1492543363365</p> <p>Data:</p> <p>id: 1128a1c6ce name: DSR-8.0.0.0.0_80.23.0.ova</p> <ol style="list-style-type: none"> 5. Cut and paste values for the <Virtual Appliance iDIH-xxx OVA ID>. <p><Virtual Appliance OVA ID> = 1128a1c6ce</p>
---	---	--

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

3 <input type="checkbox"/>	OVM-M CLI: Get the virtual appliance ID, which will be used later	<ol style="list-style-type: none"> 1. Use the site-specific value for the <Virtual Appliance iDIH-xxx OVA ID>. <Virtual Appliance iDIH-xxx OVA ID> = 1128a1c6ce 2. Copy and paste the value for <Virtual Appliance iDIH-xxx OVA ID> into the command. OVM>show VirtualAppliance id=<Virtual Appliance iDIH-xxx OVA ID> Example: OVM>show VirtualAppliance id=1128a1c6ce 3. Execute the command and validate success. 4. From the screen results, find the site specific text (highlighted). Command: show VirtualAppliance id=1128a1c6ce Status: Success Time: 2017-04-18 15:23:53,534 EDT Data: Origin = http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.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-8.0.0.0.0_80.23.0.ova] Name = DSR-8.0.0.0.0_80.23.0.ova Description = Import URL: http://10.240.155.70/iso/DSR/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova Locked = false 5. Cut and paste values for the <iDIH-xxx OVA VM name_vm_vm>. <iDIH-xxx OVA VM name_vm_vm> = 11145510c0_vm_vm
-------------------------------	---	---

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

4 <input type="checkbox"/>	OVM-M CLI: Create VM for iDIH-xxx OVA VM	<p>Create a virtual machine from the virtual machine in the OVA virtual appliance.</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <iDIH-db OVA VM name_vm_vm>. < iDIH-db OVA VM name_vm_vm > = 11145510c0_vm_vm 2. Copy and paste the value for <iDIH-db OVA VM name_vm_vm> into the command. OVM>createVmFromVirtualApplianceVm VirtualApplianceVm name=<IDIH-XXX-OVA VM name_vm_vm> Example: OVM>createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm 3. Execute the command and validate success. 4. From the screen results, find the site specific text (highlighted). Command: createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm Status: Success Time: 2016-08-30 02:15:00,859 EDT JobId: 1472537700721 Data: id: 0004fb00000600004a0e02bdf9fc1bcd name: oracle- 8.0.0.0.0_80.23.0.ova 5. Cut and paste values for the <VM ID>. <VM ID> = 0004fb00000600004a0e02bdf9fc1bcd
5 <input type="checkbox"/>	OVM-M CLI: Add VM to server pool	<ol style="list-style-type: none"> 1. Use the site-specific value for the <iDIH-db OVA VM name_vm_vm>. < iDIH-db OVA VM name_vm_vm > = 11145510c0_vm_vm 2. Copy and paste the value for <VM ID> and <Server Pool> 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" 3. Execute the command and validate success. <p>Note: Refer to E-3 Server Pool for further information.</p>

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

6	<div><div></div><div>OVM-M CLI: Edit VM to apply required profile and resources</div></div>	<div>Edit VM with required resources:</div> <div><div>1. Use the site-specific value for the <VM ID>, <VM name>, and <vCPUs Production>.</div><div><VM id> = 0004fb00000600004a0e02bdf9fc1bcd</div><div><VM name > = na-iDIH-db</div><div><vCPUs Production> = 4</div><div>Refer to Appendix C Resource Profile for recommended resource profile.</div></div> <div><table><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><tr><td>Type of guest host</td><td>#</td><td>#</td><td>#</td><td>#</td><td>#</td></tr></table></div> <div><div>2. Copy and paste the values for <VM ID>, <VM name>, <vCPUs Production> into the command.</div><div>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>"</div><div>Example:</div><div>OVM>edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=na_idih-db memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4 domainType=XEN_HVM description="na_idih-db"</div><div>3. Execute the command and validate success.</div><div>Command: edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name= na_idih-db memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4 domainType=XEN_HVM description="na_idih-db"</div><div>Status: Success</div><div>Time: 2017-04-18 17:55:25,645 EDT</div><div>JobId: 1492552525477</div><div>The VM now has a name and resources.</div></div>	VM Name	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production	Type of guest host	#	#	#	#	#
VM Name	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production									
Type of guest host	#	#	#	#	#									
7	<div><div></div><div>OVM-M CLI: Determin VNIC ID</div></div>	<div>Identify the template VNIC on the VM.</div> <div><div>1. Use the site-specific value for the <VM name>.</div><div><VM name>= na-noam-na-2a</div><div>2. Copy and paste the values for <VM name> into the command.</div><div>OVM>show Vm name=<VM name></div><div>Example:</div><div>OVM>show Vm name=na-idih-db</div><div>3. Execute the command and validate success.</div></div>												

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

		<p>4. From the screen results, find the site specific text (highlighted).</p> <pre> Command: show Vm name=NO1 Status = Stopped Memory (MB) = 6144 Max. Memory (MB) = 6144 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/8.0/ova/DSR-8.0.0.0.0_80.23.0.ova Disk Limit = 4 Huge Pages Enabled = No Config File Absolute Path = 192.168.5.5:/storage/ovm01/repository/VirtualMachines/0004fb00000600004a0e02bdf9fc1bcd/vm.cfg Config File Mounted Path = /OVS/Repositories/0004fb0000030000da5738315337bfc7/VirtualMachines/0004fb00000600004a0e02bdf9fc1bcd/vm.cfg Server Pool = 0004fb00000200009148c8926d307f05 [XLab Pool 01] Repository = 0004fb0000030000da5738315337bfc7 [XLab Utility Repo01] Vnic 1 = 0004fb0000070000091e1ab5ae291d8a [Template Vnic] VmDiskMapping 1 = 0004fb0000130000a1996c6074d40563 [Mapping for disk Id (79def426328a4127b5bf9f7ae53d3f48.img)] VmDiskMapping 2 = 0004fb00001300002db3d4b67a143ab5 [Mapping for disk Id (EMPTY_CDROM)] Restart Action On Crash = Restart Id = 0004fb00000600004a0e02bdf9fc1bcd [na-noam-na-2a] Name = na-noam-na-2a </pre>
--	--	--

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

		<div>Description = na-noam-na-2a</div> <div>Locked = false</div> <div>DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)]</div> <div>5. Cut and paste values for the <VNIC 1 ID>.</div> <div><VNIC 1 ID> = 0004fb0000070000091e1ab5ae291d8a</div>																
8	<div>Resource Profile:</div> <div>Determine network interfaces for the type of guest host</div>	<div>Refer to Appendix C Resource Profile for network interfaces to configure for each guest type.</div> <table><tr><td></td><td>OAM (XMI)</td><td>Local (IMI)</td><td>Sig A (XSI1)</td><td>Sig B (XSI2)</td><td>Sig C (XSI3-16)</td><td>Rep (SBR)</td><td>DIH Internal</td></tr><tr><td>Type of guest host</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td><td>eth#</td></tr></table> <div>Note: Create the VNICs in the correct order so the interfaces are associated with the correct network.</div>		OAM (XMI)	Local (IMI)	Sig A (XSI1)	Sig B (XSI2)	Sig C (XSI3-16)	Rep (SBR)	DIH Internal	Type of guest host	eth#	eth#	eth#	eth#	eth#	eth#	eth#
	OAM (XMI)	Local (IMI)	Sig A (XSI1)	Sig B (XSI2)	Sig C (XSI3-16)	Rep (SBR)	DIH Internal											
Type of guest host	eth#	eth#	eth#	eth#	eth#	eth#	eth#											
9	<div>OVM-M CLI:</div> <div>Attach XMI VNIC (if needed by guest host type)</div>	<div>Add (attach) VNIC ID of the XMI network to VM:</div> <div>1. Use the site-specific value for the <VNIC 1 ID> and <OVM Network ID for XMI>.</div> <div><VNIC 1 ID> = 004fb0000070000091e1ab5ae291d8a</div> <div><OVM Network ID for XMI> = 10345112c9</div> <div>2. Copy and paste the values for <VNIC 1 ID> and <OVM Network ID for XMI> into the command.</div> <div>OVM>add Vnic id=<VNIC 1 ID> to Network name=<OVM Network Id for XMI></div> <div>Example:</div> <div>OVM>add Vnic id=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9</div> <div>3. Execute the command and validate success.</div> <div>Command: add Vnic id=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9</div> <div>Status: Success</div> <div>Time: 2017-04-19 19:08:59,496 EDT</div> <div>JobId: 1492643339327</div>																

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each

10 <input type="checkbox"/>	OVM-M CLI: Create and attach iDIH internal VNIC (if needed by guest host type)	<p>Create VNIC ID on iDIH internal network and add (attach) to VM:</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <OVM Network ID for iDIH Internal> and <VM name>. <OVM Network ID for iDIH Internal> = DIH Internal <VM name> = na_idih-db 2. Copy and paste the values for <OVM Network ID for iDIH Internal> and <VM name> into the command. <pre>OVM>create Vnic network=<OVM network id for IDIH Internal> name=<VM name>-int on Vm name=<VM name></pre> <p>Example:</p> <pre>OVM>create Vnic network=DIH Internal name=na_idih-db-int on Vm name=na_idih-db</pre> 3. Execute the command and validate success. <p>Command: create Vnic network=102e89a481 name=na-noam-na-2a-IMI on Vm name=na-noam-na-2a</p> <p>Status: Success</p> <p>Time: 2017-04-19 21:21:57,363 EDT</p> <p>JobId: 1492651317194</p> <p>Data:</p> <pre>id:0004fb00000700004f16dc3bfe0750a7 name:na-noam-na-2a-IMI</pre>
11 <input type="checkbox"/>	OVM-M CLI: Create and attach IMI VNIC (if needed by guest host type)	<p>Create VNIC ID on the IMI network and attach to VM:</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <OVM Network ID for IMI> and <VM name>. <OVM Network ID for IMI> = 102e89a481 <VM name> = na-idih-db 2. Copy and paste the values for <OVM Network ID for IMI> and <VM name> into the command. <pre>OVM>create Vnic network=<OVM Network ID for IMI> name=<VM name>-IMI on Vm name=<VM name></pre> <p>Example:</p> <pre>OVM>create Vnic network=102e89a481 name=na-idih-db-IMI on Vm name=na-idih-db</pre> 3. Execute the command and validate success. <p>Command: create Vnic network=102e89a481 name=na-idih-db-IMI on Vm name=na-idih-db</p> <p>Status: Success</p> <p>Time: 2017-04-19 21:21:57,363 EDT</p> <p>JobId: 1492651317194</p> <p>Data:</p> <pre>id:0004fb00000700004f16dc3bfe0750a7 name:na-noam-na-2a-IMI</pre>

Procedure 30. (OVM-S/OVM-M Only) Import Three IDIH OVAs and Create and Configure a VM Each

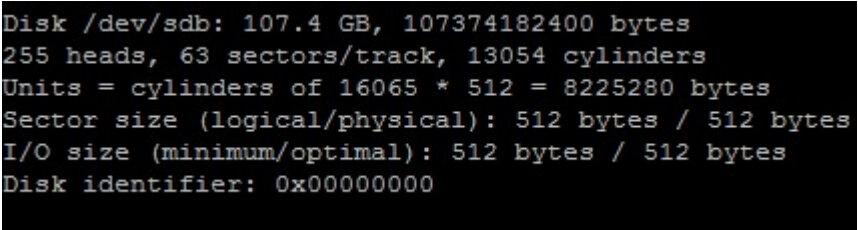
12 <input type="checkbox"/>	(iDIH Oracle VM only) OVM-M CLI: Create raw storage block device (external device)	<p>Create an extra virtual disk (only required on IDIH-Oracle (db) if the system is using OVM)</p> <ol style="list-style-type: none"> Use the site-specific value for the <VirtualDiskName>, <size in GB>, and <MyRepository name>. <VirtualDiskName> = idih-db_disk1 <size in GB> = 100 <MyRepository name> = XLab Utility Repo01 Refer to Resource Profile to learn the required GB of storage for the IDIH type: <size in GB> Copy and paste the values for <VirtualDiskName>, <size in GB>, and <MyRepository name> into the command. <pre>OVM>create VirtualDisk name='<VirtualDiskName>' size=<size in GB> sparse=<Yes/No> shareable=<Yes/No> on Repository name='<MyRepository name>'</pre> Example: <pre>OVM>create VirtualDisk name=idih-db_disk1 size=100 sparse=No shareable=No on Repository name='XLab Utility Repo01'</pre> Execute the command and validate success. From the screen results, find the site specific text (highlighted). Command: <code>create VirtualDisk name=idih-db_disk size=100 sparse=No shareable=No on Repository name='XLab Utility Repo01'</code> Status: Success Time: 2017-04-24 15:29:12,502 EDT JobId: 1493061481113 Data: id:0004fb00001200001bae7adbe6b20e19.img name:idih-db_disk Cut and paste values for the <VirtualDiskId> and <VirtualDiskName>. <VirtualDiskId> = 0004fb00001200001bae7adbe6b20e19.img <VirtualDiskName> = idih-db_disk
--------------------------------	---	---

Procedure 30. (OVM-S/OVM-M Only) Import Three iDIH OVAs and Create and Configure a VM Each


13 <input type="checkbox"/>	(iDIH Oracle VM only) OVM-M CLI: Map the create disk to a slot on the VM	<p>Map the extra virtual disk to a virtual machine disk slot.</p> <ol style="list-style-type: none"> 1. Use the site-specific value for the <Slot#>, <VirtualDiskID>, <VirtualDiskName>, and <VM name>. <Slot#> = 2 <VirtualDiskID> = 0004fb00001200001bae7adbe6b20e19.img <VirtualDiskName> = idih-db_disk <VM name> =na_idih-db 2. Copy and paste the value for <Slot#>, <VirtualDiskID>, <VirtualDiskName>, and <VM name> into the command. <pre>OVM>create VmDiskMapping slot=<Slot#> virtualDisk=<VirtualDiskId> name="<VirtualDiskName>" on Vm name=<VM name></pre> <p>Example:</p> <pre>OVM>create VmDiskMapping slot=2 virtualDisk=0004fb00001200001bae7adbe6b20e19.img name='idih-db_disk' on Vm name=na_idih-db</pre> 3. Execute the command and validate success. <p>Command: <code>create VmDiskMapping slot=2 virtualDisk=0004fb00001200001bae7adbe6b20e19.img name='idih-db_disk' on Vm name=na_idih-db</code></p> <p>Status: Success</p> <p>Time: 2017-04-24 15:32:50,875 EDT</p> <p>JobId: 1493062370724</p> <p>Data:</p> <p>id:0004fb000013000057ab9b00e6d47add name:idih-db_disk</p>
14 <input type="checkbox"/>	OVM-M CLI: Start VM	<ol style="list-style-type: none"> 1. Use the site-specific value for the <VM name>. <VM name> = na-idih-db 2. Copy and paste the value for <VM name> into the command. <pre>OVM>start Vm name=<VM name></pre> <p>Example:</p> <pre>OVM>start Vm name=na-idih-db</pre> 3. Execute the command and validate success. <p>Command: <code>start Vm name=na-idih-db</code></p> <p>Status: Success</p> <p>Time: 2017-04-19 19:29:35,376 EDT</p> <p>JobId: 1492644568558</p>
15 <input type="checkbox"/>	Procedure overview	<p>Repeat steps 1 through 14 for the following VMs. Use unique labels for the VM names:</p> <p>iDIH-Application</p> <p>iDIH-Mediation</p>

4.12. Configure iDIH Virtual Machines

Procedure 31. Configure iDIH VM Networks (Optional)

S T E P #	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 <input type="checkbox"/>	Log into the Oracle VM Console	1. Access the iDIH Oracle VM console. 2. Login as the admusr user.
2 <input type="checkbox"/>	(Oracle VM only) Verify the extra/second disk exists	<p>Note: This step is required ONLY for the Oracle VM.</p> <p>Check if the raw storage block device (external disk) exists by executing any of below commands (similar to the screenshot):</p> <pre>\$ ls /dev/[sv]db \$ sudo fdisk -l \$ df -h</pre>  <p>If the extra disk does not exist, revisit the procedures for respective hypervisors. (Procedure 28 for VMware, Procedure 29 for KVM, and Procedure 30 of OVM-M).</p> <p>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:</p> <pre>\$ df</pre> <p>If you see it has been mounted, unmount it and completely remove the entry in the /etc/fstab.</p>
3 <input type="checkbox"/>	Delete the eth0 interface	Delete the eth0 interface. <pre>\$ sudo netAdm delete -device=eth0</pre>
4 <input type="checkbox"/>	Trigger net rules file creation	Run the udevadm command to recreate net rules file. <pre>\$ sudo udevadm trigger --subsystem-match=net</pre> <p>Note: If this command does not create the net rules file, create it manually. Refer to Appendix H Sample Net Rules File.</p>

Procedure 31. Configure iDIH VM Networks (Optional)

5	<input type="checkbox"/> Modify the ethernet interface names in the net rules file	<p>Update the net rules file by replacing the default interfaces names ethX with XMI and INT interfaces names. Replace eth0 with XMI; and eth1 with INT interface. Also, update the respective MAC addresses for each interface in lowercase. MAC addresses can be determined by using the ifconfig -a command from the console.</p> <p>Note: The Mediation VM requires the user to rename a third interface: eth2 as IMI interface.</p> <p>Refer to Appendix H Sample Net Rules File for a sample net rules file.</p> <pre>\$ sudo vi /etc/udev/rules.d/70-persistent-net.rules</pre>  <p>Reboot the VM.</p> <pre>\$ sudo init 6</pre>
6	<input type="checkbox"/> As admusr on the Oracle VM configure the networks with netAdm	<p>Log into the iDIH Oracle VM console as the admusr user.</p> <ol style="list-style-type: none"> The XMI network should already exist, but it can be created with the following command. <pre>\$ sudo netAdm add --device=xmi --address=<IP Address in External Management Network> --netmask=<Netmask> --onboot=yes</pre> Configure the int network IP address and netmask. <pre>\$ sudo netAdm add --device=int --address=10.254.254.2 --netmask=255.255.255.224</pre> <p>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.</p> Mediation Only. If this is a Mediation VM, configure the Mediation internal management network. <pre>\$ sudo netAdm add --device=imi --address=<IP Address in Internal Management Network> --netmask=<Netmask></pre> Configure the default gateway. <pre>\$ sudo netAdm add --route=default --gateway=<gateway address for the External Management Network> --device=xmi</pre> <p>The VM network configuration has been completed. You should be able to ssh into the server through XMI interface.</p>

Procedure 31. Configure iDIH VM Networks (Optional)

7 <input type="checkbox"/>	As admusr on the Oracle VM configure NTP and the Oracle VM hostname	<ol style="list-style-type: none"> On the Oracle VM console, launch the platform configuration menu. <code>\$ sudo su - platcfg</code> From the platform configuration menu configure ntpserver1 with the ip address supplied for NTP Network Configuration->NTP->Edit->ntpserver1 Click Yes when asked to restart NTP. Exit the network configuration menu. Configure the Oracle VM hostname. Server Configuration->Hostname->Edit. Note: Typically, we select hostname and identify the host as iDIH application, iDIH Mediation, and iDIH Oracle. Exit the platform configuration menu.
8 <input type="checkbox"/>	Procedure overview	Repeat Steps 1 through 7 for the following VMs. Use unique labels for the VM names: iDIH Mediation iDIH Application

4.13. Post iDIH Installation Configuration**Procedure 32. Run Post Installation Scripts on iDIH VMs (Optional)**

STEP #	This procedure runs post installation scripts on the iDIH VMs. Prerequisite: Procedure 31 has been completed. 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 <input type="checkbox"/>	Log into the iDIH Oracle VM Console	<ol style="list-style-type: none"> Access the iDIH Oracle VM console. Login as the admusr user.
2 <input type="checkbox"/>	Run the iDIH Oracle post installation script	<ol style="list-style-type: none"> Wait for the software upgrades to complete on all iDIH VMs. As admusr on the iDIH Oracle VM console, run the Oracle post installation script. <code>\$ sudo /opt/xIH/oracle/configureOracle.sh</code> 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 displays without a message. Note: To verify the install status, check the <code>/var/TKLC/xIH/log/oracle/post_image_install.log</code> log file for any errors. The Cannot use backup/restore functions while using dispatcher error can safely be ignored.

Procedure 32. Run Post Installation Scripts on iDIH VMs (Optional)

3 <input type="checkbox"/>	Log into the iDIH Mediation VM Console as admusr	<ol style="list-style-type: none"> 1. Access the iDIH Mediation VM console. 2. Login as the admusr user.
4 <input type="checkbox"/>	Run the iDIH Mediation VM post installation script	<p>The Oracle post installation script must come to completion before the Mediation post installation script is run.</p> <ol style="list-style-type: none"> 1. As the admusr user on the iDIH Mediation VM console, run the Mediation post installation script. <pre>\$ sudo /opt/xIH/mediation/install.sh</pre> <p>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 log file for any error.</p> <p>Note: It is assumed network configuration and functionality is correct prior to 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:</p> <p>Log into the Mediation server as admusr.</p> <p>Execute the command sudo su - tekelec.</p> <p>Execute the command sqlplus /@NSP.</p> 2. As tekelec on the iDIH Mediation VM console, run the following commands. <pre>\$ sudo su - tekelec \$ med:/usr/TKLC/xIH iset -fnodeName=`hostname` - fhostname=`hostname` NodeInfo where 1=1</pre>
5 <input type="checkbox"/>	Log into the iDIH application VM console as admusr	<ol style="list-style-type: none"> 1. Access the iDIH Application VM console. 2. Login as the admusr user.
6 <input type="checkbox"/>	Run the iDIH Application post installation script	<p>The Mediation post installation script must come to completion before the Application post installation script is run.</p> <p>As the admusr user on the iDIH Application VM console, run the Application post installation script.</p> <pre>\$ sudo /opt/xIH/apps/install.sh</pre> <p>Note: The Application post installation script runs for 2 to 10 minutes. Wait for it to complete before the next step is executed.</p>

Procedure 32. Run Post Installation Scripts on iDIH VMs (Optional)

<div>7</div> <div><input type="checkbox"/></div>	Run the iDIH health check script on each of the iDIH VMs	<p>Once all of the iDIH VMs have restarted. Run the health check scripts on each iDIH VM.</p> <p>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.</p> <pre>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre> <p>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.</p> <pre>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre> <p>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.</p> <pre>\$ sudo /usr/TKLC/xIH/plat/bin/analyze_server.sh -i</pre> <p>Note: Ignore NTP message stating the tvoe-host is not integrated.</p>
--	--	--

Procedure 33. Configure DSR Reference Data Synchronization for iDIH (Optional)

<div>S</div> <div>T</div> <div>E</div> <div>P</div> <div>#</div>	<p>This procedure configures DSR reference data synchronization for iDIH.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
<div>1</div> <div><input type="checkbox"/></div>	iDIH Application Server: Login	<ol style="list-style-type: none"> 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. <pre>\$ sudo su - tekelec</pre>
<div>2</div> <div><input type="checkbox"/></div>	iDIH Application Server: Execute configuration script	<p>Execute the following script:</p> <pre>Apps/trda-config.sh</pre> <p>Example output:</p> <pre>corsair-app:/usr/TKLC/xIH apps/trda-config.sh dos2unix: converting file /usr/TKLC/xIH/bea/user projects/domains/tekelec/nsp/trac e-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 Copyright (c) 1982, 2014, Oracle. All rights reserved. Last Successful login time: Thu Oct 01 2015 13:27:57 - 04:00 Connected to: Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production With the Partitioning, Automatic Storage Management,</pre>


Procedure 33. Configure DSR Reference Data Synchronization for iDIH (Optional)

		<pre> 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 Produ 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 Adap [java] Task 24 completed: [Deployer:149026]stop application xIH Trace Reference Data Adap [java] Target state: stop completed on Server nsp [java] BUILD SUCCESSFUL Total time: 29 seconds Buildfile: /usr/TKLC/xIH/apps/trace-refdata- </pre>
--	--	---

Procedure 33. Configure DSR Reference Data Synchronization for iDIH (Optional)

		<pre> adapter/build.xml app.enable: common.weblogic.start: [echo] [echo] [echo] ===== [echo] application: xihtra [echo] date: 2015-10-01 15:05:10 [echo] ===== [echo] === start application EAR [echo] date: 2015-10-01 15:05:10 [java] weblogic.Deployer invoked with options: - adminurl t3://appserver:7001 - userconfigprojects/domains/tekelec/keyfile.secure -name xIH Trace Reference Data Adapter -start [java] <Oct 1, 2015 3:05:56 PM EDT> <Info> <J2EE Deployment SPI> <BEA-260121> <Initiating [java] Task 25 initiated: [Deployer:149026]start application xIH Trace Reference Data Ada [java] Task 25 completed: [Deployer:149026]start application xIH Trace Reference Data Ada [java] Target state: start completed on Server nsp [java] BUILD SUCCESSFUL Total time: 1 minute 17 seconds 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>!" </pre>
2 <input type="checkbox"/>	iDIH Application Server: Monitor completion	<p>Monitor the log file located at:</p> <pre>/var/TKLC/xIH/log/apps/weblogic/apps/application.log</pre> <p>Examine the log file for entries containing text Trace Reference Data Adapter.</p>

Procedure 34. iDIH Configuration: Configure the SSO Domain (Optional)

S T E P #	<p>This procedure configures the SSO domain for iDIH.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<div> <div> NOAM VIP GUI: Login </div> <div> <ol style="list-style-type: none"> 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. </div> </div> <div data-bbox="760 583 1133 638">  </div> <div data-bbox="521 686 745 714"> Oracle System Login </div> <div data-bbox="1125 711 1359 730"> Mon Jul 11 13:59:37 2016 EDT </div> <div data-bbox="675 770 1208 1098"> <div> <div> Log In Enter your username and password to log in </div> <div> Username: <input type="text"/> Password: <input type="password"/> <input type="checkbox"/> Change password <input type="button" value="Log In"/> </div> </div> </div> <div data-bbox="797 1110 1081 1129"> Welcome to the Oracle System Login. </div> <div data-bbox="527 1152 1357 1192"> 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. </div>

Procedure 34. iDIH Configuration: Configure the SSO Domain (Optional)

2
NOAM VIP GUI:
Configure DNS

Navigate to **Main Menu->Administration->Remote Servers->DNS Configuration**.

Select the NOAM tab.

Configure values for the following fields:

- Domain Name
- Name Server
- Search Domain 1

External DNS Name Server

	Address
Configuration Mode *	<input checked="" type="radio"/> Global <input type="radio"/> Per-site
Name Server	<input type="text"/>

Domain Search Order

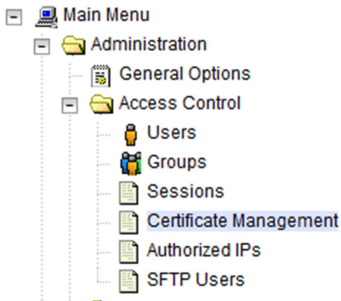

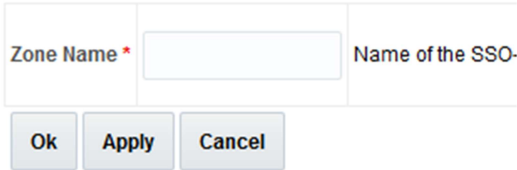

	Domain Name
Search Domain 1	<input type="text"/>
Search Domain 2	<input type="text"/>

If values have already been configured, click **Cancel**; otherwise configure the values and click **OK**.

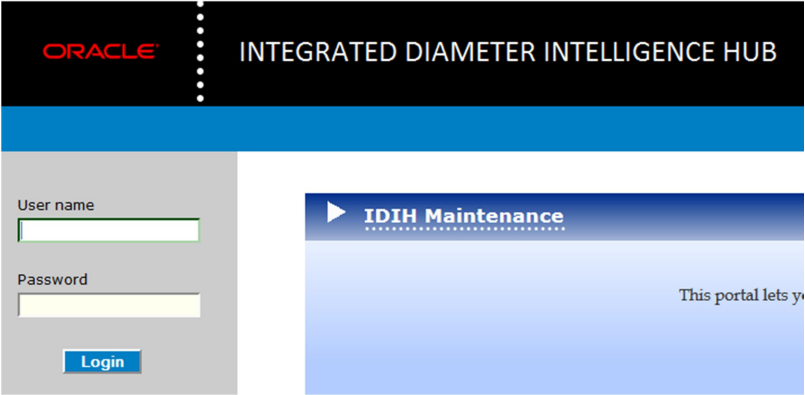
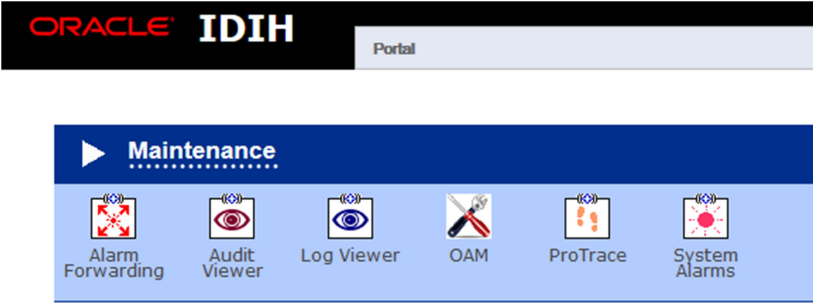
Ok

Cancel


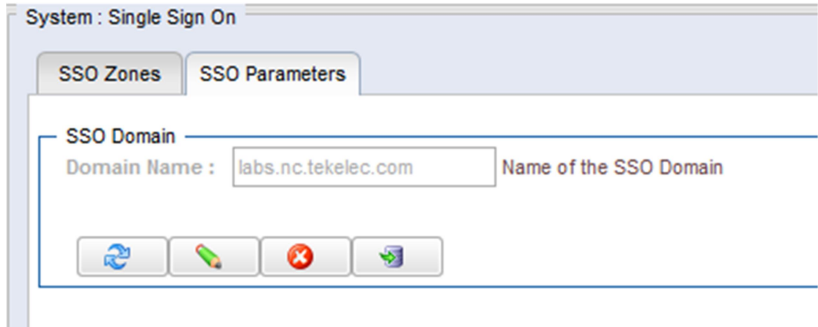
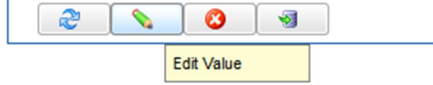

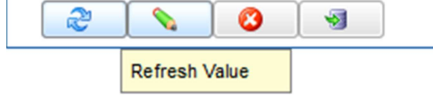
Procedure 34. iDIH Configuration: Configure the SSO Domain (Optional)

<p>3</p> <p><input type="checkbox"/></p>	<p>NOAM VIP GUI: Establish SSO local zone</p>	<p>Navigate to Main Menu->Access Control->Certification Management.</p>  <p>Click Establish SSO Zone.</p>  <p>Type a value for Zone Name.</p>  <p>Click OK.</p> <p>Information for the new certificate type of SSO local displays.</p> <p>Click Report.</p>  <p>The Certificate Report displays. Select and copy the encoded certificate text to the clipboard for future access.</p> <p>Example of Certificate Report:</p> <pre> -----BEGIN CERTIFICATE----- MIICKzCCAdWgAwIBAgIJAOVfSLnc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNV BAYTA1VTMQswCQYDVQQIDAJQZzEQMA4GA1UEBwwHUWUFSZWlnaDEPMA0GA1UECgwG T3JhY2x1MQswCQYDVQQQLDAJQVJEQMA4GA1UEAwHTGlicXJ0eTETMBEGCSqGSIb3 DQEJARYEdGVzdAeFw0xNTA1MDQxNDIzNTRaFw0xNjA1MDMxNDIzNTRaMHExCzAJ BgNVBAYTA1VTMQswCQYDVQQIDAJQZzEQMA4GA1UEBwwHUWUFSZWlnaDEPMA0GA1UE CgwGT3JhY2x1MQswCQYDVQQQLDAJQVJEQMA4GA1UEAwHTGlicXJ0eTETMBEGCSqG SIb3DQEJARYEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCZ/MpkhlvMP/iJ s5xDO2MwxJm3jYim43H8gR9pfBTMNP6L9kluJYi+2T0hngJFQLpIn6SK6pXnuAGY f/vDWfqPAgMBAAGjUDBOMB0GA1UdDgQWBBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAf BgNVHSMEGDAwBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAwBgNVHRMEBTADAQH/MA0G CSqGSIb3DQEBCwUAA0EAOwIqBMEQYvfvvt38r/yfgIx3w5dN8SBwHjHC5TpJrHV6U zFlg5dfzoLz7ditjGohWJ919VRw39LQ81KFp7SMXwA== -----END CERTIFICATE----- </pre>
--	--	---

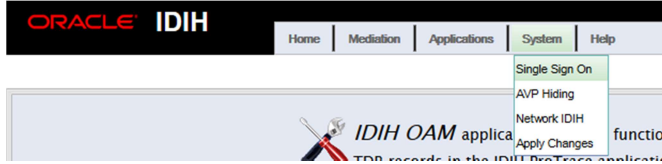
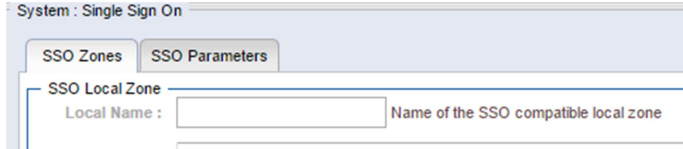
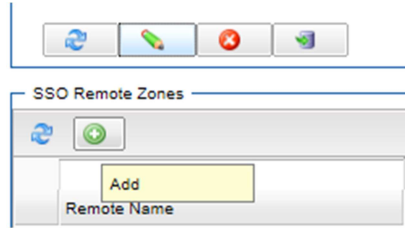
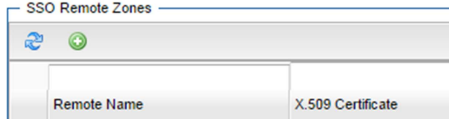
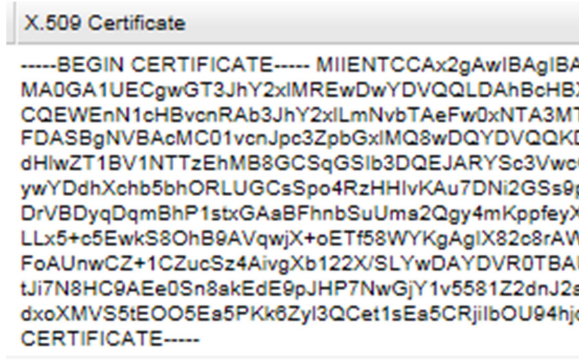


Procedure 34. iDIH Configuration: Configure the SSO Domain (Optional)

4	iDIH Application Server GUI: Login	<p>Establish a GUI session on the iDIH application server.</p> <p><a href="https://<app server IP>">https://<app server IP></p> <p>Login as the idihadmin user.</p> 
5	iDIH Application Server GUI: Launch the OAM portal	<p>Navigate to the OAM portal icon to start the OAM web application.</p> 

Procedure 34. iDIH Configuration: Configure the SSO Domain (Optional)

<p>6</p> <p><input type="checkbox"/></p> <p>iDIH Application Server GUI: Configure the SSO domain</p>	<p>Navigate to System->Single Sign On.</p>  <p>Select the SSO Parameters tab.</p>  <p>Click the Edit Value icon.</p>  <p>Type a value for the Domain Name.</p> <p>Note: This should be the same domain name assigned in the DSR NOAM DNS Configuration (step 2).</p> <p>Click the Save icon.</p>  <p>Click the Refresh icon to display data saved for the remote zone.</p> 
--	---

Procedure 34. iDIH Configuration: Configure the SSO Domain (Optional)

<p>7</p> <p><input type="checkbox"/></p> <p>iDIH Application Server GUI: Configure the SSO Remote Zone</p>	<p>Navigate to System->Single Sign On.</p>  <p>Select the SSO Zones tab.</p>  <p>Click the Add icon.</p>  <p>Type a value for field Remote Name.</p>  <p>For field X.509 Certificate, paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.</p>  <p>Click the Save icon.</p>  <p>Click the Refresh icon to display the data saved for remote zone.</p> 
---	---

Procedure 35. Integrate iDIH into DSR (Optional)

STEP#

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

Navigate to **Main Menu->Communication Agent->Configuration->Remote Servers.**

Communication Agent

Configuration

Remote Servers

Connection Groups

Routed Services

Click **Insert.**

Insert

Edit

Delete

Add the iDIH Mediation Server.

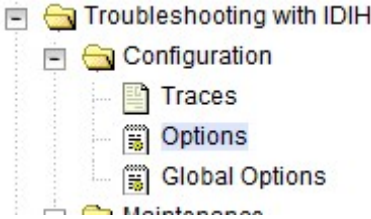
For the **Remote Server IP Address** field, type the **IMI IP address** of the iDIH Mediation server.

For the **IP Address Preference** field, select the **IP protocol preference** (if IPv6 and IPv4 are configured).

Field	Value
Remote Server Name *	<input type="text"/>
Remote Server IPv4 IP Address	<input type="text"/>
Remote Server IPv6 IP Address	<input type="text"/>
Remote Server Mode *	-- Select -- <div></div>
IP Address Preference	ComAgent Network Preference <div></div>

Set the **Remote Server Mode** to **Server.**

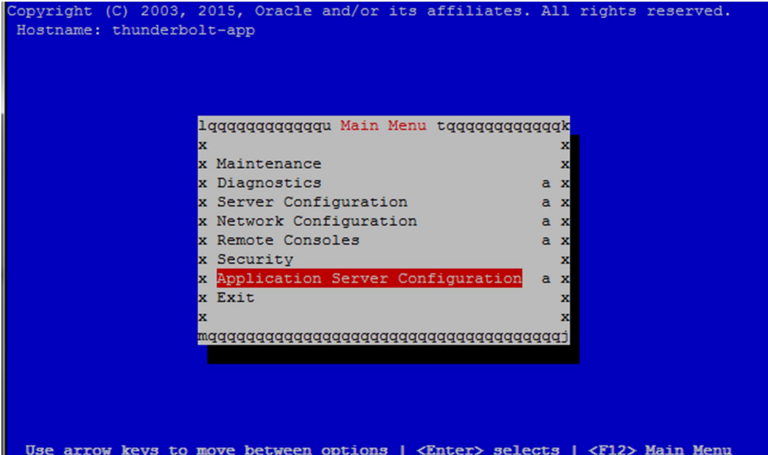
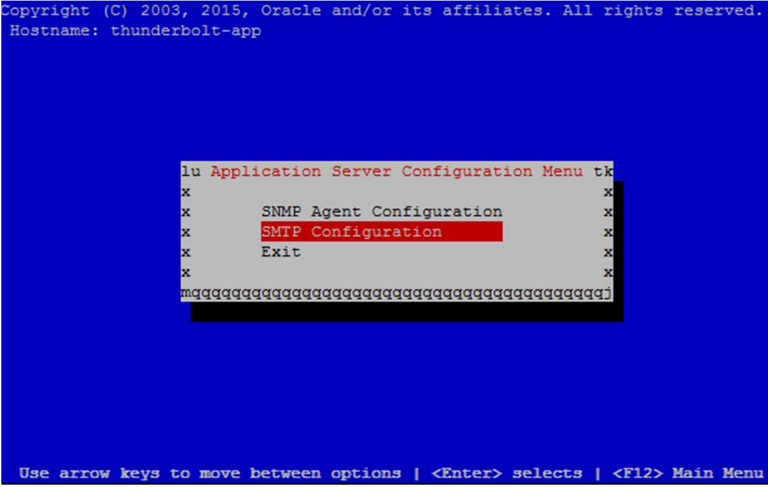
Procedure 35. Integrate iDIH into DSR (Optional)

2 <input type="checkbox"/>	Configure the Troubleshooting with iDIH on the SOAM	<p>Navigate to Main Menu->Diameter->Troubleshooting with iDIH->Configuration->Options.</p>  <p>Type the fully qualified iDIH host name (or IP address) in the iDIH Visualization Address field:</p> <p>Main Menu: Diameter -> Troubleshooting with iDIH -> Configuration -> Options</p> <table border="1" data-bbox="505 688 1209 940"> <thead> <tr> <th colspan="3">iDIH Configuration</th></tr> <tr> <th>Field</th><th>Value</th><th>Description</th></tr> </thead> <tbody> <tr> <td>Max bandwidth *</td><td>25</td><td>Maximum amount of bandwidth specified in kbps. If the bandwidth is exceeded, the peer iDIH will discard TTRs so that the bandwidth requirement is not exceeded. [Default = 25Mbps (26214400 bps); Range = 1-10000]</td></tr> <tr> <td>iDIH Host Name</td><td>Med (10.196.228.142)</td><td>The Host Name of the peer iDIH server used [Default = n/a].</td></tr> <tr> <td>iDIH Visualization address</td><td>10.240.30.150</td><td>The IP address or FQDN of the remote iDIH server. If an IP address is used in place of a FQDN, the peer iDIH must be able to resolve the IP address to a FQDN. [Default=n/a].</td></tr> </tbody> </table> <p>Apply Cancel</p> <p>Click Apply.</p>	iDIH Configuration			Field	Value	Description	Max bandwidth *	25	Maximum amount of bandwidth specified in kbps. If the bandwidth is exceeded, the peer iDIH will discard TTRs so that the bandwidth requirement is not exceeded. [Default = 25Mbps (26214400 bps); Range = 1-10000]	iDIH Host Name	Med (10.196.228.142)	The Host Name of the peer iDIH server used [Default = n/a].	iDIH Visualization address	10.240.30.150	The IP address or FQDN of the remote iDIH server. If an IP address is used in place of a FQDN, the peer iDIH must be able to resolve the IP address to a FQDN. [Default=n/a].
iDIH Configuration																	
Field	Value	Description															
Max bandwidth *	25	Maximum amount of bandwidth specified in kbps. If the bandwidth is exceeded, the peer iDIH will discard TTRs so that the bandwidth requirement is not exceeded. [Default = 25Mbps (26214400 bps); Range = 1-10000]															
iDIH Host Name	Med (10.196.228.142)	The Host Name of the peer iDIH server used [Default = n/a].															
iDIH Visualization address	10.240.30.150	The IP address or FQDN of the remote iDIH server. If an IP address is used in place of a FQDN, the peer iDIH must be able to resolve the IP address to a FQDN. [Default=n/a].															

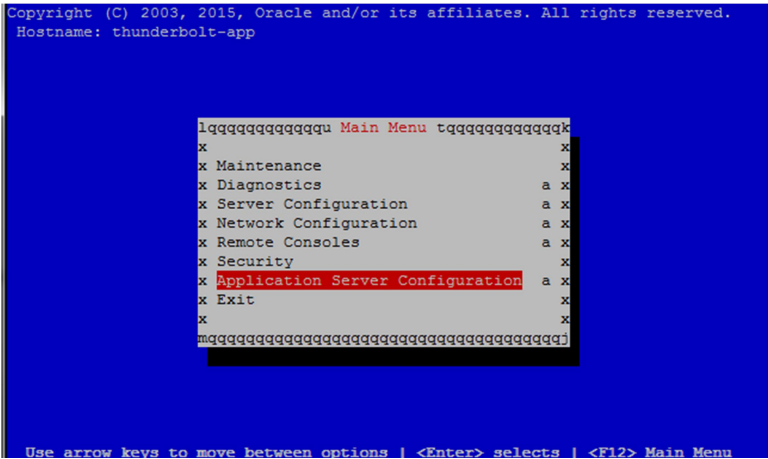
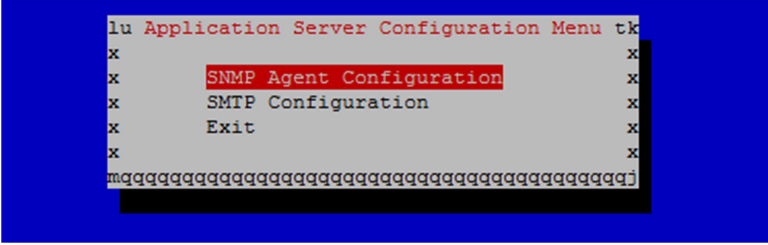
Procedure 36. iDIH Configuration: Configure the Mail Server (Optional)

S T E P #	<p>This procedure configures the SMTP mail server.</p> <p>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.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<p>iDIH Application Server: Login</p> <p>Establish an SSH session to the iDIH Application server.</p> <p>Login as the admusr user.</p>

Procedure 36. iDIH Configuration: Configure the Mail Server (Optional)

2	iDIH Application Server: Configure the authenticated mail server	<p>From the platcfg menu, type the following command:</p> <pre>\$ sudo su - platcfg</pre> <p>Select Application Server Configuration.</p>  <p>Select SMTP Configuration.</p>  <p>Select Edit.</p> <p>Enter the following parameters:</p> <ul style="list-style-type: none"> • Mail Server IP Address • User • Password • Email Address (From) • Mail smtp timeout • Mail smtp connectiontimeout • SNMP over SSL used? <p>Select OK.</p> <p>Select Exit to exit the platcfg menu.</p>
---	---	---

Procedure 37. iDIH Configuration: Configure SNMP Management Server (Optional)


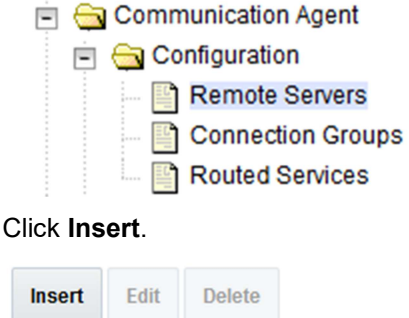
STEP #	<p>This procedure configures the SNMP management server.</p> <p>Note: This procedure is optional; however, this option is required for forwarding (forwarding by SNMP filter defined), and is available only on the Application server.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	iDIH Application Server: Login	<p>Establish an SSH session to the iDIH Application server.</p> <p>Login as the admusr user.</p>
2 <input type="checkbox"/>	iDIH Application Server: Configure the authenticated mail server	<p>From the platcfg menu, type the following command:</p> <pre>\$ sudo su - platcfg</pre> <p>Select Application Server Configuration.</p>  <p>Select SNMP Agent Configuration.</p>  <p>Select Edit.</p> <p>Enter the IP Address of the SNMP management server.</p> <p>Note: The SNMP agent configuration is updated and the SNMP management server automatically restarts.</p> <p>Select OK.</p> <p>Select Exit to exit the platcfg menu.</p>

Procedure 38. iDIH Configuration: Change Network Interface (Optional)

S T E P #	<p>This procedure changes the default network interface.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<p>iDIH Mediation Server: Login</p> <p>Establish an SSH session to the iDIH Mediation server.</p> <p>Login as the admusr user.</p> <p>Type the following command to login in as the Tekelec user.</p> <pre>\$ sudo su - tekelec</pre>
2 <input type="checkbox"/>	<p>iDIH Mediation Server: Execute the change interface script</p> <p>To execute the change interface script, type the following command:</p> <pre>\$ chgIntf.sh</pre> <p>Answer the questions during the script as follows.</p> <p>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.</p> <p>Current setting are: interface.name=imi interface.enabled=True</p> <p>Enter new network interface name, return to keep current [imi]: xmi</p> <p>Do you want to enable network interface filtering [True False], return to keep current [True]:</p> <p>Updating configuration properties file with 'interface.name=xmi' and 'interface.enable=True', and restarting mediation configuration bundle...</p>

4.14. Post-Install Activities

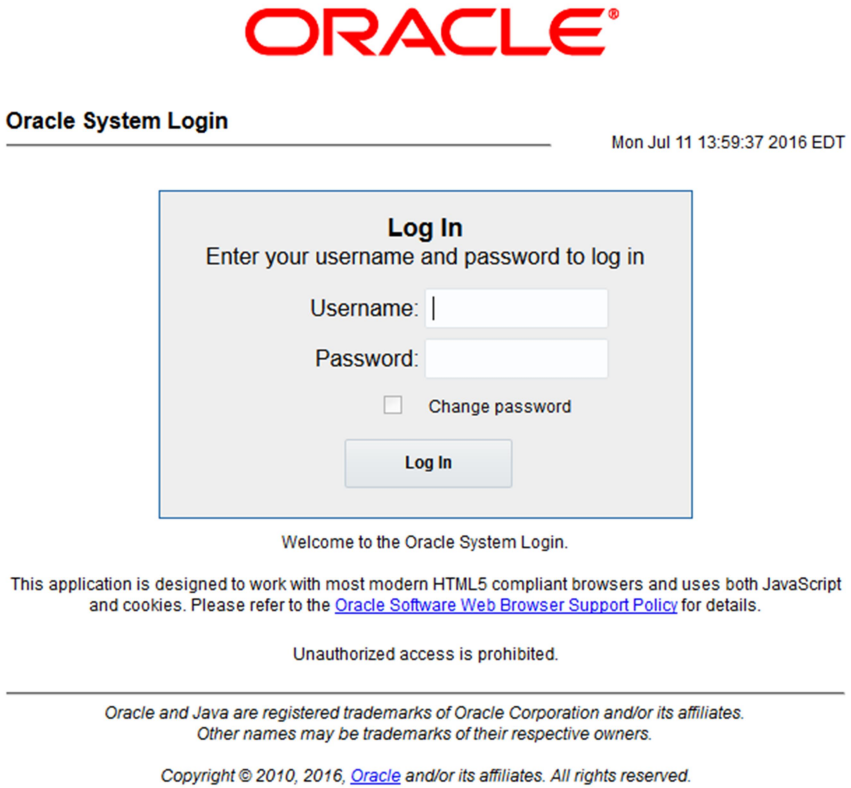
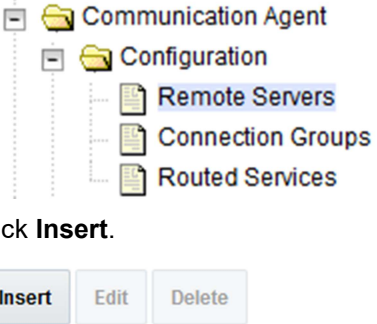
Procedure 39. Configure ComAgent Connections

S T E P #	<p>This procedure configures ComAgent connections on DSR for use in the FABR application.</p> <p>Prerequisite: FABR application is activated.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>
1 <input type="checkbox"/>	<p>SDS NOAM VIP GUI: Login</p> <ol style="list-style-type: none"> 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. 
2 <input type="checkbox"/>	<p>SDS NOAM VIP GUI: Configure remote server IP address</p> <p>Navigate to Main Menu->Communication Agent->Configuration->Remote Servers.</p>  <p>Click Insert.</p>



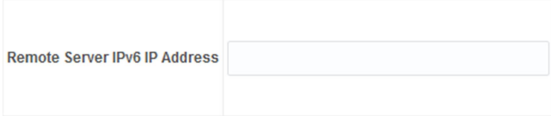
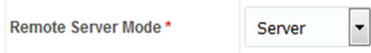
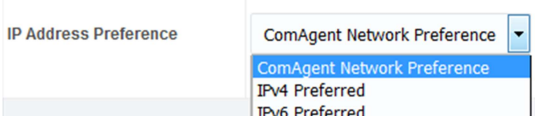
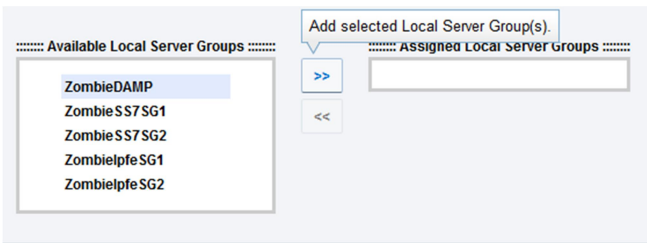

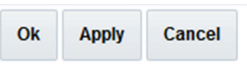
Procedure 39. Configure ComAgent Connections

3 <input type="checkbox"/>	SDS NOAM VIP GUI: Configure remote server IP address	<p>Type Remote Server Name for the DSR MP server.</p> <p>Remote Server Name * <input type="text" value="ZombieDAMP1"/></p> <p>Type the Remote Server IMI IP address.</p> <p>Remote Server IPv4 IP Address <input type="text" value="169.254.1.13"/></p> <p>Remote Server IPv6 IP Address <input type="text"/></p> <p>Note: This should be the IMI IP address of the DAMP server.</p> <p>Select Client for the Remote Server Mode from the list.</p> <p>Remote Server Mode * <input type="text" value="Client"/></p> <p>Select IP Address Preference (ComAgent Network Preference, IPv4, or IPv6) from the list.</p> <p>IP Address Preference <input type="text" value="ComAgent Network Preference"/></p> <p>Select the Local Server Group from the available SDS DP server groups and click >> to assign.</p> <p>Available Local Server Groups: <input type="text" value="SDSDP"/> >> Assigned Local Server Groups: <input type="text"/></p> <p>Available Local Server Groups: <input type="text"/> >> Assigned Local Server Groups: <input type="text" value="SDSDP"/></p> <p>Click Apply.</p> <p>Ok Apply Cancel</p>
4 <input type="checkbox"/>	SDS NOAM VIP GUI: Repeat	Repeat steps 2-3 for each remote MP in the same SOAM NE.

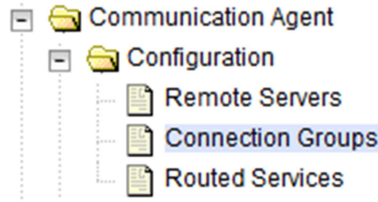
Procedure 39. Configure ComAgent Connections

4 <input type="checkbox"/>	DSR NOAM VIP GUI: Login	<ol style="list-style-type: none"> 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 https://<Primary_DSR_NOAM_VIP_IP_Address> as the URL 2. Login as the guiadmin user. 
6 <input type="checkbox"/>	DSR NOAM VIP GUI: Configure remote server IP address	<p>Navigate to Main Menu->Communication Agent->Configuration->Remote Servers.</p> 

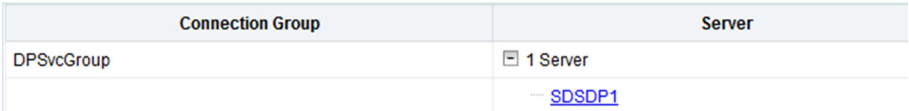
Procedure 39. Configure ComAgent Connections

<p>7</p> <p><input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Configure remote server IP address</p>	<p>Type Remote Server Name for the DSR MP server.</p>  <p>Type the Remote Server IMI IP address.</p>   <p>Note: This should be the IMI IP address of the DP server.</p> <p>Select Server for the Remote Server Mode from the list.</p>  <p>Select IP Address Preference (ComAgent Network Preference, IPv4, or IPv6) from the list.</p>  <p>Select the Local Server Group from the available DSR MP server groups and click >> to assign.</p>   <p>Click Apply.</p> 
<p>8</p> <p><input type="checkbox"/></p>	<p>DSR NOAM VIP GUI: Repeat</p>	<p>Repeat steps 6-7 for each remote DP in the same SOAM NE.</p>

Procedure 39. Configure ComAgent Connections

9	DSR NOAM VIP GUI: Configure connection groups	<p>Navigate to Main Menu->Communication Agent->Configuration->Connection Groups.</p> 																
9	DSR NOAM VIP GUI: Edit connection groups	<p>Select the DPSvcGroup connection group.</p> <table border="1"> <thead> <tr> <th>Connection Group</th><th>Server</th></tr> </thead> <tbody> <tr> <td>DPSvcGroup</td><td>0 Servers</td></tr> </tbody> </table> <p>Click Edit</p> <p>Select the DP Servers from the Available Servers in Network Element list and click >> to assign.</p> <p>Editing existing Connection Groups</p> <table border="1"> <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: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]</td></tr> </tbody> </table> <div> <div>Available Servers in Network Element</div> <div>SDSDP1</div> <div>>></div> <div><<</div> <div>Assigned Servers in Connection Group</div> <div></div> </div> <p>Editing existing Connection Groups</p> <table border="1"> <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: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]</td></tr> </tbody> </table> <div> <div>Available Servers in Network Element</div> <div></div> <div>>></div> <div><<</div> <div>Assigned Servers in Connection Group</div> <div>SDSDP1</div> </div> <p>Click OK.</p> <div> <div>Ok</div> <div>Apply</div> <div>Cancel</div> </div>	Connection Group	Server	DPSvcGroup	0 Servers	Field	Value	Description	Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]	Field	Value	Description	Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]
Connection Group	Server																	
DPSvcGroup	0 Servers																	
Field	Value	Description																
Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]																
Field	Value	Description																
Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid character alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]																

Procedure 39. Configure ComAgent Connections

11 <input type="checkbox"/>	DSR NOAM VIP GUI: Verify servers in group	Verify the correct number of servers are in the connection group. 
--------------------------------	--	---

Procedure 40. Complete PCA Configuration (Optional)

STEP #	This procedure completes PCA configuration. Prerequisite: PCA 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.	
1 <input type="checkbox"/>	Complete PCA configuration	Refer to PCA Configuration section in [2] DSR PCA Activation Guide, E81528 for the steps required to complete PCA configuration.

Procedure 41. Backups and Disaster Prevention

STEP #	This procedure provides instruction on backups and disaster prevention. Prerequisite: DSR and optional sub-systems are installed configured. 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 <input type="checkbox"/>	Backups	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.

Procedure 42. (KVM/OpenStack Only) Configure Port Security

STEP #	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 section G-6 in Appendix G 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.	
1 <input type="checkbox"/>	IPFE with TSA only. Remove port security on TSA XMI network interfaces on IPFE and MP instances	If using IPFE with target set addresses. 1. Determine the TSA IP address as used in section 4.7, i.e., Procedure 20, steps 2. 2. Determine the corresponding XSI interface IP address as used in section 4.7, i.e., Procedure 20, steps 2.

Procedure 42. (KVM/OpenStack Only) Configure Port Security

	<p>3. Log into the OpenStack control node as the admusr user.</p> <p>4. Source the tenant user credentials.</p> <p>5. Determine security groups associated with the IPFE instance.</p> <pre>\$ nova list-secgroup <VM instance ID></pre> <p>Note: <VM instance ID> can be queried from the output of nova list command in the ID column for the given VM.</p> <p>6. Save the ID and names of the listed security groups for later use.</p> <p>7. Remove all listed security groups.</p> <pre>\$ nova remove-secgroup <VM instance ID> <Security group ID></pre> <p>Note: Use the <VM instance ID> and <Security group ID> as noted down in the step-6 above.</p> <p>Alternatively, we can use the following syntax:</p> <pre>\$ nova remove-secgroup <VM instance name> <Security group name></pre> <p>8. Determine the port ID of the XSI interface IP address from step 2 above.</p> <pre>\$ neutron port-list -F id -F fixed_ips grep <instance IP on TSA/XSI network></pre> <p>Note: <port ID> is the value in first column of the output to this command.</p> <p>9. Disable port security for the port found in step 7.</p> <pre>\$ neutron port-update <Port ID> --port-security-enabled=false</pre> <p>10. Re-enable port security for all the interfaces not on the TSA/XSI port used in step 9, including XMI, IMI, and others.</p> <p>Determine the port IDs of the instance IP addresses not associated with the TSA/XSI network.</p> <pre>\$ neutron port-list -F id -F fixed_ips grep <instance IP not on TSA/XSI network></pre> <p>For each of the non TSA/XSI instance ports perform the following command for each of the security groups from step 6.</p> <pre>\$ neutron port-update <Port ID> --security-group <Security group ID>></pre> <p>Note: Use the <Security Group ID> as noted in the step 6 above.</p>
--	--

Procedure 43. Enable/Disable DTLS (SCTP Diameter Connections Only)

S T E P #	<p>This procedure prepares clients before configuring SCTP Diameter connections.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Enable/Disable DTLS (SCTP Diameter connections only)	<p>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.</p> <p>https://access.redhat.com/security/cve/CVE-2015-1421</p> <p>https://access.redhat.com/security/cve/CVE-2014-5077</p> <p>Execute procedures in [22] DSR DTLS Feature Activation Procedure, E78942 to disable/enable the DTLS feature.</p>

Procedure 44. Shared Secret Encryption Key Revocation (RADIUS Only)

S T E P #	<p>This procedure changes the shared secret encryption key on DSR RADIUS setup.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Revoke RADIUS shared secret encryption key	<p>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.</p> <p>Note: It is highly recommended to change the key after installation due to security reasons.</p>

Procedure 45. DSR Performance Tuning

S T E P #	<p>This procedure changes tuning parameters for the system to achieve better performance.</p> <p>Check off (✓) each step as it is completed. Boxes have been provided for this purpose under each step number.</p> <p>If this procedure fails, contact My Oracle Support (MOS) and ask for assistance.</p>	
1 <input type="checkbox"/>	Performance tuning (Optional)	Refer to Appendix I Performance Tuning Recommendations 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 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

Time Zone Value	Description	Universal Time Code (UTC) Offset
America/New_York	Eastern Time	UTC-05
America/Chicago	Central Time	UTC-06
America/Denver	Mountain Time	UTC-07
America/Phoenix	Mountain Standard Time — Arizona	UTC-07
America/Los Angeles	Pacific Time	UTC-08
America/Anchorage	Alaska Time	UTC-09
Pacific/Honolulu	Hawaii	UTC-10
Africa/Johannesburg		UTC+02

Time Zone Value	Description	Universal Time Code (UTC) Offset
America/Mexico City	Central Time — most locations	UTC-06
Africa/Monrovia		UTC+00
Asia/Tokyo		UTC+09
America/Jamaica		UTC-05
Europe/Rome		UTC+01
Asia/Hong Kong		UTC+08
Pacific/Guam		UTC+10
Europe/Athens		UTC+02
Europe/London		UTC+00
Europe/Paris		UTC+01
Europe/Madrid	mainland	UTC+01
Africa/Cairo		UTC+02
Europe/Copenhagen		UTC+01
Europe/Berlin		UTC+01
Europe/Prague		UTC+01
America/Vancouver	Pacific Time — west British Columbia	UTC-08
America/Edmonton	Mountain Time — Alberta, east British Columbia & west Saskatchewan	UTC-07
America/Toronto	Eastern Time — Ontario — most locations	UTC-05
America/Montreal	Eastern Time — Quebec — most locations	UTC-05
America/Sao Paulo	South & Southeast Brazil	UTC-03
Europe/Brussels		UTC+01
Australia/Perth	Western Australia — most locations	UTC+08
Australia/Sydney	New South Wales — most locations	UTC+10
Asia/Seoul		UTC+09
Africa/Lagos		UTC+01
Europe/Warsaw		UTC+01
America/Puerto Rico		UTC-04
Europe/Moscow	Moscow+00 — west Russia	UTC+04
Asia/Manila		UTC+08
Atlantic/Reykjavik		UTC+00
Asia/Jerusalem		UTC+02

Appendix C. Resource Profile

VM Name	VM Purpose	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production	Notes
DSR NOAM	Network Operation, Administration, and Maintenance	2	4	4	6	70	
DSR SOAM	Site Operation, Administration and Maintenance	2	4	4	6	70	
DA MP	Diameter Agent Message Processor	2	9 (24 for IWF)	12	16 (24 for IWF)	70	The 24 GB RAM requirement is a minimum if the DA-MP VM will be used with the IWF.
IPFE	IP Front End			6	16	70	
SS7 MP	SS7 Message Processor for MAP Diameter			8	24	70	The 24 GB RAM requirement is a hard minimum for SS7
SBR(s)	Subscriber Binding Repository (session) for Policy DRA			12	25	70	To support 5M sessions
SBR(b)	Subscriber Binding Repository (binding) for Policy DRA			12	32	70	
iDIH Application	Integrated Diameter Intelligence Hub web server			4	8	64	
iDIH Mediation	Integrated Diameter Intelligence Hub mediation server			4	8	64	

VM Name	VM Purpose	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production	Notes
iDIH DB	Integrated Diameter Intelligence Hub DB server			4	8	120(system) + 100 (DB)	Storage for DB Disk may be increased

VM Name	OAM (XMI)	Local (IMI)	Signaling A (XSI1)	Signaling B (XSI2)	Signaling C (XSI3)	Signaling D (XSI4)	Replication (SBR Rep)	DIH Internal
DSR NOAM	eth0	eth1						eth0
DSR SOAM	eth0	eth1						eth0
DA-MP	eth0	eth1	eth2	eth3	eth4-17	eth18		eth0
IPFE	eth0	eth1	eth2	eth3	eth4-17			eth0
SS7 MP	eth0	eth1	eth2	eth3	eth4-17	eth18		eth0
SBRB	eth0	eth1				eth2		eth0
SBRS	eth0	eth1				eth2		eth0
iDIH App	xmi						int	xmi
iDIH Med	xmi	imi					int	xmi
iDIH DB	xmi						int	xmi

Note: The Ethernet interfaces defined in the table are there as a guideline. Interfaces can be ordered as preferred, i.e., eth1 or eth2 could be associated with XMI if desired.

Appendix D. Common KVM/Openstack Tasks

Procedure D-1. Create a Network Port

1 <input type="checkbox"/>	Create the network ports for the NO network interfaces	<ol style="list-style-type: none"> Each network interface on an instance must have an associated network port. An instance usually has at least eth0 and eth1 for a public and private network respectively. Some configurations require 6 or more interfaces and corresponding network ports. 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 Identify the neutron network ID associated with each IP/interface using the neutron command line tool. <code>\$ neutron net-list</code> Identify the neutron subnet ID associated with each IP/interface using the neutron command line tool. <code>\$ neutron subnet-list</code> 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. <code>\$. keystone_rc_dsr_user</code> <code>\$ keystone user-list</code> <code>\$ neutron port-create --name=NO1-xmi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=10.x.x.157 <network id></code> <code>\$ neutron port-create --name=NO1-imi --tenant-id <tenant id> --fixed-ip subnet_id=<subnet id>,ip_address=192.168.x.157 <network id></code> View your newly created ports using the neutron tool. <code>\$ neutron port-list</code>
-------------------------------	--	--

Procedure D-2. Create and Boot OpenStack Instance

1 <input type="checkbox"/>	Create a VM instance from a glance image	<ol style="list-style-type: none"> 1. Get the following configuration values. The image ID. <pre>\$ glance image-list</pre> The flavor ID. <pre>\$ nova flavor-list</pre> The network ID(s) <pre>\$ neutron net-list</pre> An informative name for the instance. NO1 SO2 MP5 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. The number of IP/interfaces for each VM type must conform with the interface-to-network mappings described at the bottom of Appendix C Resource Profile. Note: IPv6 addresses should use the v6-fixed-ip argument instead of v4-fixed-ip. <pre>\$ 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</pre> View the newly created instance using the nova tool. <pre>\$ nova list --all-tenants</pre> 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.
-------------------------------	--	---

Procedure D-3. Configure Networking for OpenStack Instance

1 <input type="checkbox"/>	Verify/Configure the network interface	<p>Check if interface is configured automatically.</p> <p>If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address. To verify, ping the XMI IP address provided with nova boot... command:</p> <pre>\$ping <XMI-IP-Provided-During-Nova-Boot></pre> <p>If the ping is successful, ignore the next part to configure the interface manually.</p> <p>Manually configure the interface, if not already done (Optional)</p> <ol style="list-style-type: none"> 1. Log into the Horizon GUI as the DSR tenant user. 2. Go to the Compute/Instances section. 3. Click on 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 to the interface-to-network mappings described at the bottom of the Resource Profile in Appendix C. <pre>\$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask></pre> <pre>\$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip></pre> <p>Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.</p> <ol style="list-style-type: none"> 7. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting. <pre>\$ sudo init 6</pre> <p>The new VM should now be accessible via both network and Horizon console.</p>
-------------------------------	--	---

Appendix E. Common OVM-Manager Tasks (CLI)

E-1. Set 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.

Procedure E-1. Set Up Server

1 <input type="checkbox"/>	Log into the OVM-M command line interface	<pre>Ssh -l admin <OVM-M IP> -p 1000</pre> <p>Example:</p> <pre>[root@manager01 ~]# ssh -l admin 10.240.16.138 -p 10000</pre> <p>admin@10.240.16.138's password:</p>
2 <input type="checkbox"/>	OVM-M CLI: Discover Oracle VM server	<pre>discoverServer ipAddress=value password=value takeOwnership= { Yes No }</pre> <p>Example:</p> <pre>OVM>discoverServer ipAddress=10.240.16.139 password=password takeOwnership=Yes</pre>
3 <input type="checkbox"/>	OVM-M CLI: Create an ethernet-based network with the VM role	<pre>create Network [roles= { MANAGEMENT LIVE_MIGRATE CLUSTER_HEARTBEAT VIRTUAL_MACHINE STORAGE }] name=value [description=value] [on Server instance]</pre> <p>Example:</p> <pre>OVM>create Network name=XMI roles=VIRTUAL_MACHINE</pre>
4 <input type="checkbox"/>	OVM-M CLI: Add a port from each Oracle VM server to the network	<p>Note: Skip this step and proceed to step 5 for bonded interfaces.</p> <ol style="list-style-type: none"> Find the ID of an Ethernet port. <pre>OVM> show Server name=MyServer1</pre> <pre>...</pre> <pre>Ethernet Port 1 = 0004fb00002000007711332ff75857ee [eth0 on MyServer3.virtlab.info]</pre> <pre>Ethernet Port 2 = 0004fb0000200000d2e7d2d352a6654e [eth1 on MyServer3.virtlab.info]</pre> <pre>Ethernet Port 3 = 0004fb0000200000c12192a08f2236e4 [eth2 on MyServer3.virtlab.info]</pre> <pre>...</pre> Add a port from each Oracle VM Server to the network. <pre>OVM>add Port instance to { BondPort Network } instance</pre> <p>Example:</p> <pre>OVM>add Port id=0004fb0000200000d2e7d2d352a6654e to Network name=MyVMNetwork</pre>

Procedure E-1. Set Up Server

5 <input type="checkbox"/>	OVM-M CLI: Create Bondport (For Bonded Interfaces)	<ol style="list-style-type: none"> Find the ID of an Ethernet port. OVM><code>list Port</code> Status: Success Time: 2016-08-22 04:43:02,565 EDT Data: id:0004fb0000200000045b4e8dc0b3acc6 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:0004fb0000200000247b03c2a4a090ec name:eth1 on vms01.test.com Create Bondport on required interfaces. OVM><code>create BondPort ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server name=compute01.test.com</code> Command: create BondPort ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server name=compute01.test.com Status: Success
6 <input type="checkbox"/>	OVM-M CLI: Add VLAN Interface to network (for VLAN tagged networks)	<ol style="list-style-type: none"> Find the ID of an Ethernet port. OVM><code>list BondPort</code> 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 Create VLAN interface. OVM><code>create VlanInterface vlanId=43 name=bond1.43 on BondPort id=0004fb00002000005a45a0761813d512</code>

Procedure E-1. Set Up Server

		<p>Command: create VlanInterface vlanId=43 name=bond1.43 on BondPort id=0004fb00002000005a45a0761813d512</p> <p>Status: Success</p> <p>3. Add remaining VLAN interfaces to the same bond accordingly, like:</p> <p>OVM>create VlanInterface vlanId=44 name=bond1.44 on BondPort id=0004fb00002000005a45a0761813d512</p> <p>OVM>create VlanInterface vlanId=30 name=bond1.30 on BondPort id=0004fb00002000005a45a0761813d512</p> <p>OVM>create VlanInterface vlanId=31 name=bond1.31 on BondPort id=0004fb00002000005a45a0761813d512</p> <p>4. Add VLAN interfaces to network.</p> <p>OVM>add VlanInterface name=bond1.43 to Network name=XMI</p> <p>Command: add VlanInterface name=bond1.43 to Network name=XMI</p> <p>Status: Success</p> <p>Time: 2016-08-22 05:14:29,321 EDT</p> <p>JobId: 1471857258238</p> <p>OVM>add VlanInterface name=bond1.44 to Network name=IMI</p> <p>Command: add VlanInterface name=bond1.44 to Network name=IMI</p> <p>Status: Success</p> <p>Time: 2016-08-22 05:15:24,216 EDT</p> <p>JobId: 1471857321329</p> <p>OVM>add VlanInterface name=bond1.30 to Network name=XSI1</p> <p>Command: add VlanInterface name=bond1.30 to Network name=XSI1</p> <p>Status: Success</p> <p>Time: 2016-08-22 05:15:39,190 EDT</p> <p>JobId: 1471857337005</p> <p>OVM>add VlanInterface name=bond1.31 to Network name=XSI2</p> <p>Command: add VlanInterface name=bond1.31 to Network name=XSI2</p> <p>Status: Success</p> <p>Time: 2016-08-22 05:15:52,576 EDT</p> <p>JobId: 1471857349684</p>
--	--	---

Procedure E-1. Set Up Server

7 <input type="checkbox"/>	OVM-M CLI: Create unclustered server pool	Note: To create clustered server pool, ignore this step and proceed to next. OVM> <code>create ServerPool clusterEnable=No name=MyServerPool description='Unclustered server pool'</code>
8 <input type="checkbox"/>	OVM-M CLI: Create clustered server pool (Optional)	Note: Skip this step if an unclustered server pool is already created. This step is only if required to create a clustered server pool. 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> <code>list FileSystem</code> id:66a61958-e61a-44fe-b0e0-9dd64abef7e3 name:nfs on 10.172.76.125:/mnt/vol1/poolfs03 id:0004fb0000050000b85745f78b0c4b61 name:fs on 350014ee2568cc0cf id:4ebb1575-e611-4662-87b9-a84b40ce3db7 name:nfs on 10.172.76.125:/mnt/vol1/poolfs04 id:858d98c5-3d8b-460e-9160-3415cbdda738 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-0a96-4845-9690-740bbf1e225e 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:0004fb000005000006a46a8dbd2461939 name:MyServerPool_cluster_heartbeat id:0004fb00000500000809e28f4fab56b1 name:fs on 350014ee20137ee44 OVM> <code>list PhysicalDisk</code> id:0004fb000018000019b86ccf3f473a9e name:FreeBSD (9) id:0004fb0000180000c4609a67d55b5803 name:FreeBSD (3) id:0004fb00001800002179de6afe5f0cf3 name:SATA_WDC_WD5001ABYS-_WD-WCAS86288968 id:0004fb0000180000a0b43f9684fc78ac name:FreeBSD (2) id:0004fb0000180000732be086afb26911 name:FreeBSD (7) id:0004fb000018000067ce80973e18374e name:FreeBSD (8) id:0004fb000018000035ce16ee4d58dc4d name:FreeBSD (1) id:0004fb00001800006855117242d9a537 name:FreeBSD (6) id:0004fb0000180000a9c7a87ba52ce5ec name:FreeBSD (5) id:0004fb0000180000ebabef9838188d78 name:SATA_WDC_WD5001ABYS-_WD-WCAS86571931

Procedure E-1. Set Up Server

		<pre>id:0004fb00001800008f6ea92426f2cfb8 name:SATA_WDC_WD5001ABYS-_WD-WCAS86257005 id:0004fb00001800008ccb1925cdbbd181 name:SATA_WDC_WD5001ABYS-_WD-WCAS86578538 id:0004fb0000180000e034b4662665161c name:FreeBSD (4)</pre> <p>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:</p> <pre>OVM>refresh { AccessGroup Assembly FileServer FileSystem PhysicalDisk Repository Server StorageArray VirtualAppliance } instance</pre> <p>For example, to refresh a physical disk:</p> <pre>OVM>refresh PhysicalDisk id=0004fb000018000035ce16ee4d58dc4d</pre> <p>3. Refresh a file system:</p> <pre>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'</pre>
9	OVM-M CLI: Add Oracle VM servers to the server pool	<pre>OVM>add Server name=MyServer to ServerPool name=MyServerPool</pre>
10	OVM-M CLI: Create storage repository	<p>1. Find the physical disk (LUN) to use for creating the storage repository.</p> <pre>OVM>list FileServer</pre> <p>Command: list FileServer</p> <p>Status: Success</p> <p>Time: 2016-08-19 02:11:39,779 EDT</p> <p>Data:</p> <pre>id:0004fb00000900000445dac29e88bc38 name:Local FS vms03.test.com id:0004fb0000090000045715cad6f165ecf name:Local FS vms01.test.com id:0004fb00000900000df4cd9c3170092e4 name:Local FS vms02.test.com id:0004fb0000090000064b96ed88a9a0185 name:Local FS vms04.test.com</pre> <p>2. Find a local file system on an Oracle VM server that has access to the LUN.</p> <pre>OVM>list FileServer</pre> <p>Command: list FileServer</p> <p>Status: Success</p>

Procedure E-1. Set Up Server

		<p>Time: 2016-08-19 02:11:39,779 EDT</p> <p>Data:</p> <p>id:0004fb00000900000445dac29e88bc38 name:Local FS vms03.test.com</p> <p>id:0004fb0000090000045715cad6f165ecf name:Local FS vms01.test.com</p> <p>id:0004fb00000900000df4cd9c3170092e4 name:Local FS vms02.test.com</p> <p>id:0004fb0000090000064b96ed88a9a0185 name:Local FS vms04.test.com</p> <p>3. Create file system.</p> <p>OVM>create FileSystem name=VmsFs01 physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e 490ac3f392" on FileServer name="Local FS vms01.test.com"</p> <p>Command: create FileSystem name=VmsFs01 physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e 490ac3f392" on FileServer name="Local FS vms01.test.com"</p> <p>Status: Success</p> <p>Time: 2016-08-19 02:22:46,581 EDT</p> <p>JobId: 1471587738752</p> <p>Data:</p> <p>id:0004fb000005000006779d42da60c0be6 name:VmsFs01</p> <p>4. Create repository.</p> <p>OVM>create Repository name=Vms01Repo on FileSystem name=VmsFs01</p> <p>Command: create Repository name=Vms01Repo on FileSystem name=VmsFs01</p> <p>Status: Success</p> <p>Time: 2016-08-19 02:24:04,092 EDT</p> <p>JobId: 1471587843432</p> <p>Data:</p> <p>id:0004fb000003000003c8f771791114d53 name:Vms01Repo</p> <p>OVM></p> <p>Add serverpool to repository</p> <p>OVM> add ServerPool name=TestPool001 to Repository name=Vms01Repo</p> <p>Refresh the storage repository using the syntax:</p> <p>OVM> refresh Repository name=MyRepository</p>
--	--	--

E-2. Create a VM

Procedure E-2. Create a VM

1 <input type="checkbox"/>	OVM-M CLI: Import the OVA	<p>1. Import the virtual appliance/OVA.</p> <pre>OVM>importVirtualAppliance Repository name=MyRepository url="http:///example.com//myvirtualappliance.ova"</pre> <p>Example:</p> <pre>OVM>importVirtualAppliance Repository name=Vms01Repo url=http:///10.240.191.134//DSR-8.0.0.0.0_80.11.0.ova</pre> <p>Command: importVirtualAppliance Repository name=Vms01Repo url=http:///10.240.191.134//DSR- 8.0.0.0.0_80.11.0.ova</p> <p>Status: Success</p> <p>Time: 2016-09-09 07:33:11,777 EDT</p> <p>JobId: 1473420749759</p> <p>Data:</p> <p>id: 11cdf999eb name:DSR-8.0.0.0.0_80.11.0.ova</p> <p>Note: Use the highlighted ID for referring to the newly created virtual appliance in any further commands.</p>
-------------------------------	-------------------------------------	--

Procedure E-2. Create a VM

2 <input type="checkbox"/>	OVM-M CLI: Create VM	<ol style="list-style-type: none"> 1. Show virtual appliance to get the VM ID. Note: The ID referred to in the following command is the virtual appliance ID from the above step. <pre>OVM>show VirtualAppliance id=11cdf999eb</pre> Command: show VirtualAppliance id=11cdf999eb Status: Success Time: 2016-09-09 07:39:12,491 EDT Data: Origin = http:///10.240.191.134//DSR-8.0.0.0.0_80.11.0.ova Repository = 0004fb000003000072973b7457792d93 [Vms01Repo] Virtual Appliance Vm 1 = 11cdf999eb_vm_vm [vm] Virtual Appliance VirtualDisk 1 = 11cdf999eb_disk_disk1 [disk1] Id = 11cdf999eb [DSR-8.0.0.0.0_80.11.0.ova] Name = DSR-8.0.0.0.0_80.11.0.ova Description = Import URL: http:///10.240.191.134//DSR-8.0.0.0.0_80.11.0.ova Locked = false 2. Create a VM from a virtual machine in a virtual appliance. Note: The virtual appliance VM name referred in the below command is the name from the above step. <pre>OVM>createVmFromVirtualApplianceVm VirtualApplianceVm name= 11cdf999eb_vm_vm</pre> Command: createVmFromVirtualApplianceVm VirtualApplianceVm name=11cdf999eb_vm_vm Status: Success Time: 2016-09-09 07:53:05,702 EDT JobId: 1473421832449 Data: id:0004fb000006000009a08ec97ad5496b name:DSR-8.0.0.0.0_80.11.0.ova_vm
-------------------------------	--------------------------------	--

Procedure E-2. Create a VM

3 <input type="checkbox"/>	OVM-M CLI: Add VM to server pool	1. Add VM to server pool. OVM>add Vm instance to { AntiAffinityGroup Server ServerPool } instance Example: OVM>add Vm id=0004fb000006000009a08ec97ad5496b to ServerPool name=TestPool001 Command: add Vm id=0004fb000006000009a08ec97ad5496b to ServerPool name=TestPool001 Status: Success Time: 2016-08-30 02:15:00,859 EDT JobId: 1472537700721 Note: Refer E-3 Server Pool section for further information on Server Pool.
4 <input type="checkbox"/>	OVM-M CLI: Edit VM with required profile/resource	1. Edit VM with required resources. Refer Appendix C Resource Profile for recommended resource profile. Note: Use the VM ID/Name in any related commands. OVM>edit Vm id=0004fb000006000009a08ec97ad5496b name=NO1 memory=24584 memoryLimit=24584 cpuCountLimit=8 cpuCount=8 domainType= XEN_HVM description="NO1" Command: edit Vm id=0004fb000006000009a08ec97ad5496b name=NO1 memory=24584 memoryLimit=24584 cpuCountLimit=8 cpuCount=8 domainType= XEN_HVM description="NO1" Status: Success Time: 2016-08-22 02:04:09,329 EDT JobId: 1471845849193
5 <input type="checkbox"/>	OVM-M CLI: Attach VNIC	1. If VNIC is already created, attach it. First, get the VNIC ID: OVM>show Vm name=NO1 Command: show Vm name=NO1 Status: Success Time: 2016-08-24 06:42:00,115 EDT Data: Status = Running Memory (MB) = 6584 Max. Memory (MB) = 6584 Processors = 6 Max. Processors = 6 Priority = 50 Processor Cap = 100 High Availability = No

Procedure E-2. Create a VM

		<pre> Operating System = Oracle Linux 6 Mouse Type = PS2 Mouse Domain Type = Xen HVM PV Drivers Keymap = en-us Start Policy = Use Pool Policy Origin = http://10.240.191.134/DSR-8.0.0.0.0_80.8.0.ova Disk Limit = 107 Huge Pages Enabled = No Config File Absolute Path = /dev/mapper/OVM_SYS_REPO_PART_3600605b00a15b2601cb8a56a 1410036a/VirtualMachines/0004fb0000060000e07023e7051a92 3c/vm.cfg Config File Mounted Path = /OVS/Repositories/0004fb000003000072973b7457792d93/Virt ualMachines/0004fb0000060000e07023e7051a923c/vm.cfg Server = 08:00:20:ff:ff:ff:ff:ff:ff:ff:00:10:e0:71:91:34 [compute01.test.com] Server Pool = 0004fb0000020000ff238819a2310353 [TestPool001] Repository = 0004fb000003000072973b7457792d93 [Vms01Repo] Vnic 1 = 0004fb000007000078f3fdb5bea01697 [00:21:f6:6f:b6:b1] VmDiskMapping 1 = 0004fb0000130000ac3e9f3d21e90188 [Mapping for disk Id (0004fb0000120000c95393297e1028e9.img)] VmDiskMapping 2 = 0004fb00001300002852a93587c1893a [Mapping for disk Id (EMPTY_CDROM)] Restart Action On Crash = Restart Id = 0004fb0000060000e07023e7051a923c [NO1] Name = NO1 Description = DSR NO1 Locked = false DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)] OVM>list Network Command: list Network Status: Success Time: 2016-09-26 05:34:25,088 EDT Data: </pre>
--	--	---

Procedure E-2. Create a VM

		<pre>id:109560cfdc name:XSI1 id:10e361d8ee name:XSI2 id:107561a2ba name:XMI id:10333df5b6 name:IMI id:0af01080 name:10.240.16.128</pre>
6 <input type="checkbox"/>	OVM-M CLI: Create and attach remaining VNICS for the VM	<p>Create VNIC on the network and attach to it.</p> <p>Note: The network referred to in the following command is the network name from the above step.</p> <pre>OVM>create Vnic network=IMI name=NO1-IMI on Vm name=NO1</pre> <p>Command: create Vnic network=IMI name=NO1-IMI on Vm name=NO1Status: Success</p> <p>Time: 2016-08-22 05:38:34,252 EDT</p> <p>JobId: 1471858714114</p> <p>Data:</p> <pre>id:0004fb0000070000b51a093ec88ed87d name: NO1-IMI</pre> <p>Note: Repeat this step for all required interfaces (XSI1, XS2 etc.). Create VNICS in the correct order so the interfaces are associated with the correct network.</p>
7 <input type="checkbox"/>	OVM-M CLI: Start VM	<pre>OVM>start Vm name=NO1</pre> <p>Command: start Vm name=NO1</p> <p>Status: Success</p> <p>Time: 2016-08-22 06:32:37,853 EDT</p> <p>JobId: 1471861954163</p>

Procedure E-2. Create a VM

8	OVM-M CLI: Configure instance networking	<ol style="list-style-type: none"> 1. Log into the OVM-M GUI/console. <a href="https://<OVM-M-IP:port>/ovm/console/faces/login.jspx">https://<OVM-M-IP:port>/ovm/console/faces/login.jspx 2. Go to the servers and VMs tab. 3. Select the host from the Server Pools. 4. Go to Virtual Machines, select the VM, and click Launch Console. 5. Login as the admusr user. 6. Configure the required network interfaces, conforming to the interface-to-network mappings described at the bottom of Appendix C Resource Profile. <pre>\$ sudo netAdm set --onboot=yes --device=eth0 --address=<xmi ip> --netmask=<xmi net mask></pre> <pre>\$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway ip></pre> Verify network connectivity by pinging Gateway of XMI network. <pre>\$ ping -c3 <XMI Gateway></pre> 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. <pre>\$ sudo init 6</pre> The new VM should now be accessible via both network and console.
---	--	--

E-3. 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, E64081 for more information.

Appendix F. Firewall Ports

Flow Description	Purpose	Protocol/Port	IP Protocol Version
ICMP echo to OA	plat management	ICMP	IPv4, IPV6
OpenHPI MGMT and Communication	plat management	TCP:443	IPv4, IPVv6
virtual guest discovery via libvirt	control	TCP:22	IPv4 , IPv6
NTP flow for time sync	plat management	UDP:123	IPv4 , IPv6
SSH & SFTP access into PM&C	plat management	TCP:22	IPv4 , IPv6
PM&C GUI Access	plat management	TCP: 80 TCP: 443	IPv4, IPv6
Server Install (time)	control	TCP:37	IPv4
Server Install (http)	control	TCP: 80	IPv4
Server Install (SNMP)	control	UDP:162	IPv4 , IPv6

Flow Description	Purpose	Protocol/Port	IP Protocol Version
Server Upgrade (nfs)	control	UDP: 111 TCP: 886 TCP: 2049 UDP/TCP: 4000-4003	IPv4
NTP flow for time sync	control	UDP:123	IPv4 , IPv6
hostname resolution (dns)	plat management	UDP/TCP: 53	IPv4, IPv6
LightWeight Directory Access Protocol (LDAP)	plat management	UDP/TCP: 389	IPv4, IPv6

Appendix G. Application VIP Failover Options (OpenStack)

G-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 the following figure:

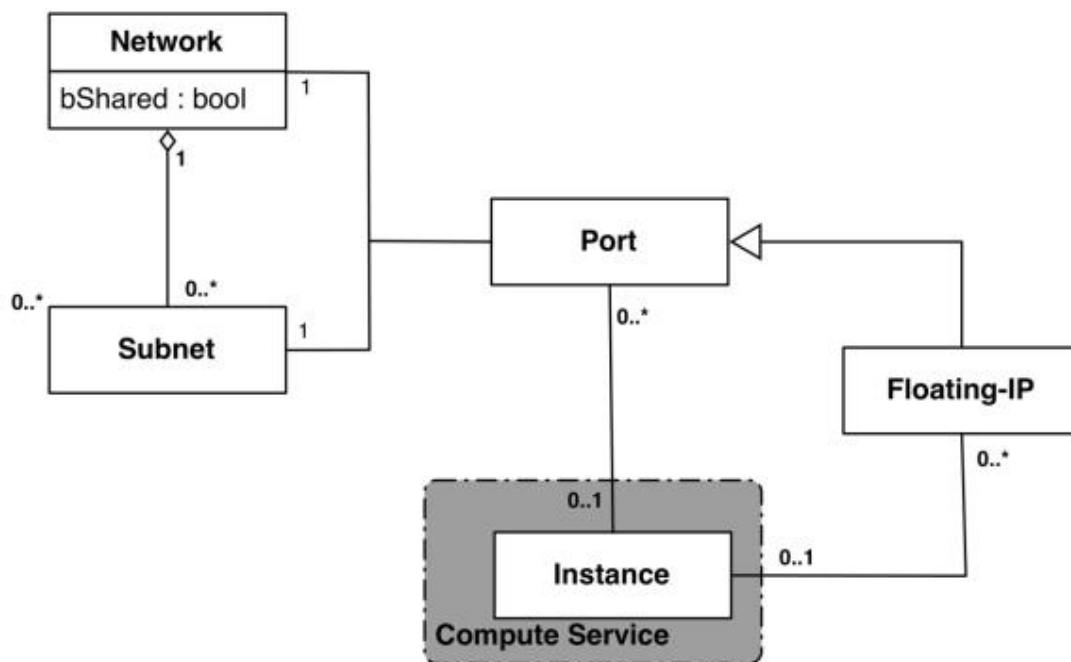


Figure 2. Neutron High-Level Data Model

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.

G-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 utilize this option after a VM instance has already booted, and how to utilize this option before a VM instance has booted.

G-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
```

alias	name
security-group	security-group
l3_agent_scheduler	L3 Agent Scheduler
net-mtu	Network MTU
ext-gw-mode	Neutron L3 Configurable external gateway mode
binding	Port Binding
provider	Provider Network
agent	agent
quotas	Quota management support
subnet_allocation	Subnet Allocation
dhcp_agent_scheduler	DHCP Agent Scheduler
l3-ha	HA Router extension
multi-provider	Multi Provider Network
external-net	Neutron external network
router	Neutron L3 Router
allowed-address-pairs	Allowed Address Pairs
extraroute	Neutron Extra Route
extra_dhcp_opt	Neutron Extra DHCP opts
dvr	Distributed Virtual Router

The allowed-address-pairs extension should appear in the list of extensions as shown in the bold line above.

G-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:

```
# neutron port-update <Port ID> --allowed_address_pairs list=true
type=dict ip_address=<VIP address to be added>
```

where the variables 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-7fc94211277 then you would type the following command:

```
# neutron port-update 8a440d3f-4e5c-4ba2-9e5e-7fc942111277 --
allowed_address_pairs list=true type=dict ip_address=10.133.97.136/30
```

G-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:

```
# 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 variables 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.

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
-f value -F id ext-subnet),ip_address=10.133.97.133 $(neutron net-show -f
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 -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.

G-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, simply disables 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.

The three sub-sections that follow describe the OpenStack configuration requirements for this option, how to utilize this option after a VM instance has already booted, and how to use this option before a VM instance has booted.

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.

G-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-secgroup <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:

```
# nova remove-secgroup <VM instance name> <Security group name>
```

where the variables have 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:

```
# nova remove-secgroup 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:

```
# neutron port-update <Port ID> -- port-security-enabled=false
```

where the variable 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:

```
# 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.

G-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:

```
# 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 variables 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:

```
# 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:

```
# 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.

G-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:

```
# 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 H. Sample Net Rules File

Udev uses rules files that determine how it identifies devices and creates device names. The udev daemon (udev) 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.

```
# eth2 interface with MAC address "fa:16:3e:8a:1a:12" will be assigned
"imi"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="*",
ATTR{address}=="fa:16:3e:8a:1a:12", ATTR{dev_id}=="0x0"
ATTR{type}=="1", KERNEL=="eth*", NAME="imi"
```

Notes:

1. The 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 interface names as in the above example.

Appendix I. Performance Tuning Recommendations

I.1. KVM/OpenStack

For the DSR system to achieve 50K MPS or more through IPFE, a few tuning parameters need to be changed.

txqueuelen

Turn on the compute hosts.

Purpose: Default value of 500 is too small. Our recommendation is to set to 30000 to increase 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

Turn 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]

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>
```

I.2. VMWare

txqueuelen

Turn on the ESXi hosts.

Purpose: Default value of 500 is too small. Our recommendation is to set to 10000 to increase the network throughput of a VM. ESXi defaults the value to 500 permits a maximum value of 10000.

How/What to Change: Log into the cli console of the ESX host and execute the following command:

```
# esxcli system settings advanced set -i=10000 -
o=/Net/MaxNetifTxQueueLen
```

Ring Buffer Increase on the Physical Ethernet Interfaces

Turn 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 maximum value for both is 4096.

How/What to Change: Log into the cli console of the ESX host and execute the following commands:

```
#esxcli 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.

Ring Buffer Increase on the Physical Ethernet Interfaces

Turn on the 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 following commands:

```
#esxcli system settings advanced set -i=0 -
o=/Numa/SwapLoadEnable
#esxcli system settings advanced set -i=0 -
o=/Numa/SwapLocalityEnable
```


Appendix J. My Oracle Support (MOS)

MOS (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at **1-800-223-1711** (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

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.