Oracle® Communications

DSR Cloud Installation Guide

Release 9.2.0.0.0

G43630-01

September 2025

Oracle Communications DSR Cloud Installation Guide, Release 9.2.0.0.0

G43630-01

Contents

1 Introduction

2 Installation

3 Software Installation Procedure

4 Software Installation Using HEAT Templates (OpenStack)

5 Application Configuration

6 Postinstallation Activities

A Sample Network Element and Hardware Profiles

Preface

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

My Oracle Support

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

Call the Customer Access Support 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 My Oracle Support, select **2**.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Acronyms

An alphabetized list of acronyms used in the document.

Table Acronyms

Acronym	Definition
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
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 (for example, 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
vSTP	Virtual Signaling Transfer Point

What's New in This Guide

This section introduces the documentation updates for release 9.2.0.0.0.

Release 9.2.0.0.0 - G43630-01, September 2025

- Added the Workaround for Configuring GUI and MMI Using Label Format for FQDN/Realm section for the users who prefer to continue with label format for GUI and MMI configurations.
- Volume support is removed in the IDIH Deployment Using VNFM section.
- Added step 3 and 6 in the Multiqueue on IPFE (KVM) appendix.
- Added the following features in the IDIH Deployment Using VNFM section:
  - IDIH Deployment on KVM with RAW Images
  - IDIH Raw Setup
  - IDIH Deployment on OpenStack with RAW Images
  - IDIH Deployment on Oracle Cloud Infrastructure (OCI) with RAW Images

1 Introduction

This document describes the procedures to install the Diameter Signaling Router (DSR) 9.2.0.0.0 and the compatible IDIH applications on a supported Cloud platform.

It is assumed that the platform-related configuration has already been done.

The audience for this document includes Oracle customers and the Software System, Product Verification, Documentation, and Customer Service including Software Operations and First Office Application groups.

1.1 References

- *Communication Agent Configuration Guide*
- *DSR PCA Activation Guide*
- *DSR Meta Administration Feature Activation Procedure*
- *DSR Full Address Based Resolution (FABR) Feature Activation Procedure*
- *DSR Range Based Address Resolution (RBAR) Feature Activation*
- *SDS SW Installation and Configuration Guide*
- *Operations, Administration, and Maintenance (OAM) User’s Guide*
- *Communication Agent User’s Guide*
- *Diameter User’s Guide*
- *Mediation User’s Guide*
- *Range Based Address Resolution (RBAR) User’s Guide*
- *Full Address Based Resolution (FABR) User’s Guide*
- *IP Front End (IPFE) User’s Guide*
- *DSR Alarms and KPIs Reference*
- *Measurements Reference*
- *Diameter Common User’s Guide*
- *DSR Security Guide*
- *DSR IPv6 Migration Guide*
- *DSR DTLS Feature Activation Procedure*
- *DSR RADIUS Shared Secret Encryption Key Revocation MOP MO008572*
- *DCA Framework and Application Activation and Deactivation Guide*
- *Oracle VM Concepts Guide, Release 3.4*
- *Networking v2.0 API documentation*
- *DSR Cloud Benchmarking Guide*
- *DSR Cloud Upgrade Guide*

1.2 Terminology

Table 1-1 Terminology

Term	Definition
Site	Applicable for various applications, a site is type of **place**. A place is configured object that allows servers to be associated with a physical location. A site place allows servers to be associated with a physical site. For example, sites may be configured for Atlanta, Charlotte, and Chicago. Every server is associated with exactly one site when the server is configured. For the Policy and Charging DRA application, when configuring a site, only put DA-MPs and SBR MP servers in the site. Do not add NOAM, SOAM, or IPFE MPs to a site.
Place Association	Applicable for various applications, a **Place Association** is a configured object that allows places to be grouped together. A place can be a member of more than one place association. The Policy and Charging DRA application defines two place association types: policy binding region and Policy and Charging mated sites.
Policy and Charging SBR Server Group Redundancy	The Policy and Charging application use SBR server groups to store the application data. The SBR server groups support both two and three site redundancies. The server group function name is **Policy and Charging SBR**.
Server Group Primary Site	A server group primary site is a term used to represent the principle location within a SOAM or SBR server group. SOAM and SBR server groups are intended to span several sites (places). For the Policy and Charging DRA application, these sites (places) are all configured within a single **Policy and Charging Mated Sites** place association. For the Diameter custom application, these sites (places) are configured in **Applications Region** place association. The primary site may be in a different site (place) for each configured SOAM or SBR server group. A primary site is described as the location in which the active and standby servers reside. However, there cannot be any preferred spare servers within this location. All SOAM and SBR server groups have a primary site.
Server Group Secondary Site	A server group secondary site is a term used to represent location in addition to the Primary Site within a SOAM or SBR Server Group. SOAM and SBR server groups are intended to span several sites (places). For the Policy and Charging DRA application, these sites (places) are all configured within a single **Policy and Charging Mated Sites** place association. For the Diameter custom application, these sites (places) are configured in **Applications Region** place association. The secondary site may be in a different site (places) for each configured SOAM or SBR server group. A secondary site is described as the location in which only preferred spare servers reside. The active and standby servers cannot reside within this location. If two site redundancy is wanted, a secondary site is required for all SOAM and SBR server groups.
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 redundancies. The server group function name is **Session and Binding Repository**.

Table 1-1 (Cont.) Terminology

Term	Definition
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 and 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

Installation

This section provides a brief overview of the recommended methods for installing the source release software, which is installed and running on a Cloud, to the target release software.

2.1 Prerequisites

Following are the prerequisites for installation:

- One target release DSR OVA Media
- Three iDIH OVA (Optional iDIH):
  - Service OVA
  - Kafka OVA
  - MySQL Server OVA

2.2 Overview

This section describes the overall strategy to follow for a single or multi-site DSR and iDIH installation. It lists the procedures required for installation with estimated times and discusses the overall installation strategy and includes an installation flowchart to determine exactly which procedures should be run for an installation. This section details the steps required to install a DSR system.

Additionally, basic firewall port information is included in the Firewall Ports section. Some procedures are cloud platform dependent and not all of these procedures are performed on cloud platforms.

2.2.1 Installation Strategy

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

- An overall installation requirement is decided upon the following data:
  - 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?
  - If the SNMP traps be viewed at the NOAM or if an external NMS can be used or in some cases both.
- A site survey (NAPD) is conducted with the customer to determine exact networking and site details.

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

DSR currently supports the following installation strategies:

- **DSR installation without using HEAT templates**
  DSR Single Site Installation Procedure Map Without Using HEAT Templates figure illustrates the overall process that each DSR installation involves. In summary, this involves creation of guests and configures each guest role based on Resource Profile and Configure Network.

Table 2-1 DSR Single Site Installation Procedure Map Without Using HEAT Templates

VM Ware	KVM/OS	OVM-S/OVM-M
Installing DSR on OL8 and KVM	NA	NA
Creating and Installing OCDSR VMs through KVM GUI	NA	NA
Importing DSR OVA (VMware)	NA	Create DSR Guests (OVM-S/OVM-M)
Configuring NOAM Guests Role Based On Resource Profile and Configure Network (VMware)	Configure NOAM Guests Role Based on Resource Profile (KVM/OpenStack Only)	Configure Virtual Machines (OVM-S/OVM-M)
Configure Remaining DSR Guests Based on Resource Profile and Configure Network	Configure Remaining DSR Guests Based on Resource Profile and Configure Network (KVM/OpenStack Only)	NA
Install DSR on Oracle Linux/KVM	NA	NA
Create and Install DSR VMs through KVM GUI	NA	NA
Prepare OpenStack Template and Environment Files	NA	NA
Create OpenStack Parameter File for NOAM	NA	NA
Create OpenStack Parameter File for Signaling	NA	NA
Application Configuration	NA	
Configure the Signaling Network Routes	NA	NA
Configure DSCP Values for Outgoing Traffic	NA	NA
Configure IP Front End	NA	NA
SNMP Configuration	NA	NA
iDIH Configuration to Configure the SSO Domain	NA	NA
Configure ComAgent Connections	NA	NA
Complete PCA Configuration	NA	NA
Backups and Disaster Prevention	NA	NA
Configure Port Security (KVM/OpenStack Only)	NA	NA
Enable/Disable DTLS (SCTP Diameter Connections Only)	NA	NA
Shared Secret Encryption Key Revocation (RADIUS Only)	NA	NA

Table 2-1 (Cont.) DSR Single Site Installation Procedure Map Without Using HEAT Templates

VM Ware	KVM/OS	OVM-S/OVM-M
DSR Performance Tuning	NA	NA
Change NOAM/SOAM Profile for Increased MP Capacity on a Virtualized Environment	NA	NA
Create a Network Port	NA	NA
Create and Boot OpenStack Instance	NA	NA
Configure Networking for OpenStack Instance	NA	NA
Set Up the Server	NA	NA
Scale a Signaling Node	NA	NA
Multiqueue on IPFE (KVM)	NA	NA

- **DSR installation using HEAT templates (OpenStack)**
  DSR Installation Procedure Map Using HEAT Templates figure illustrates the overall process that each DSR installation involves using the Heat Templates. It involves creation of parameter files, environment files, template files, DSR Topology Configuration xml and deploys DSR using OpenStack CLI commands.

Table 2-2 DSR Single Site Installation Procedure Map Using HEAT Templates

Sequence	Openstack Cloud Platform
1	Install DSR on Oracle Linux/KVM
2	Deploy HEAT Templates
3	Application Configuration
4	Configure the Signaling Network Routes
5	If DSCP is used, perform Configure DSCP Values for Outgoing Traffic. If not, move to next step.
6	Configure IP Front End
13	iDIH Configuration to Configure the SSO Domain

2.2.2 SNMP Configuration

The network-wide plan for SNMP configuration should be finalized before DSR installation proceeds. This section provides 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:

- Send all their SNMP traps to the NOAM by merging them 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.
- Send all their SNMP traps to an external Network Management Station (NMS). The traps are seen at the SOAM and NOAM as alarms. They are viewable at the configured NMS(s) as traps.

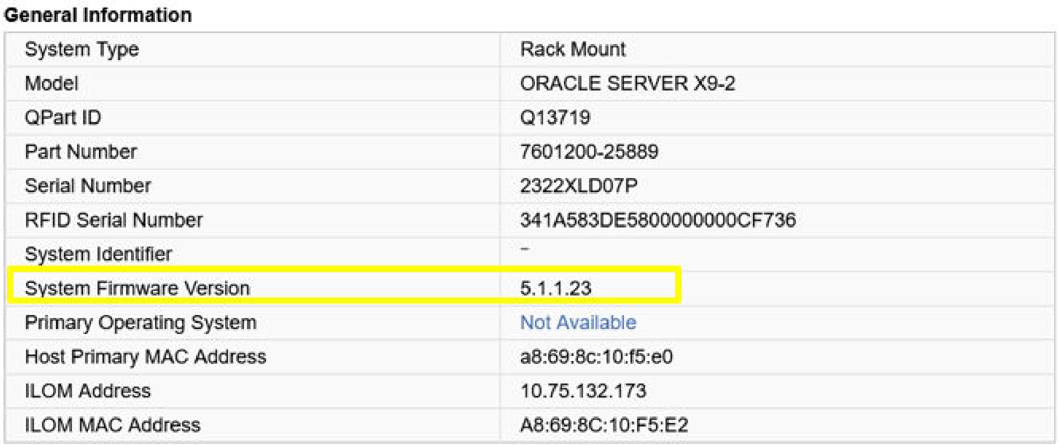
Application server SNMP configuration is done from the NOAM GUI at the end of DSR installation.

2.3 Verifying the Hardware Configuration

Perform the following procedure to verify hardware configuration.

1. Log in to the latest **iLOM GUI**

Figure 2-1   iLOM GUI



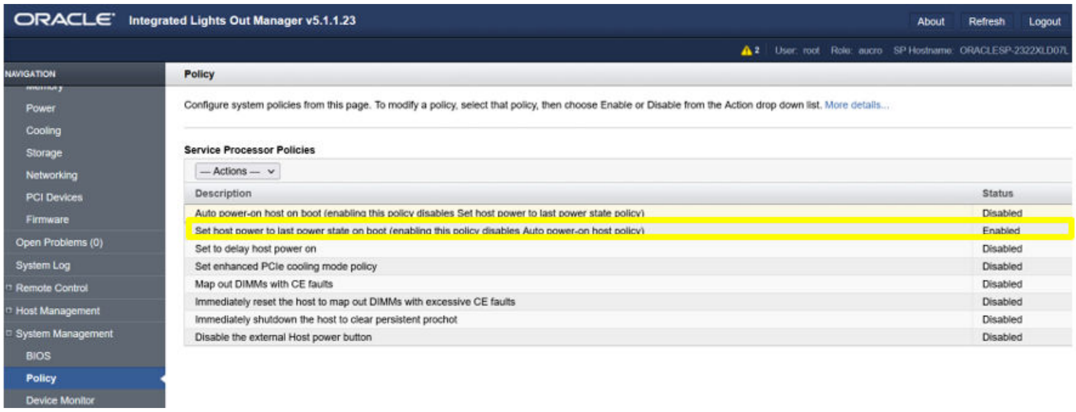
General Information

System Type	Rack Mount
Model	ORACLE SERVER X9-2
QPart ID	Q13719
Part Number	7601200-25889
Serial Number	2322XLD07P
RFID Serial Number	341A583DE5800000000CF736
System Identifier	-
System Firmware Version	5.1.1.23
Primary Operating System	Not Available
Host Primary MAC Address	a8:69:8c:10:f5:e0
ILOM Address	10.75.132.173
ILOM MAC Address	A8:69:8C:10:F5:E2

2. Verify if the last power state of iLOM is enabled:

   Go to `iLOM/Web-System Management/Policy`

Figure 2-2   Verify power state



Policy

Configure system policies from this page. To modify a policy, select that policy, then choose Enable or Disable from the Action drop down list. More details...

Service Processor Policies

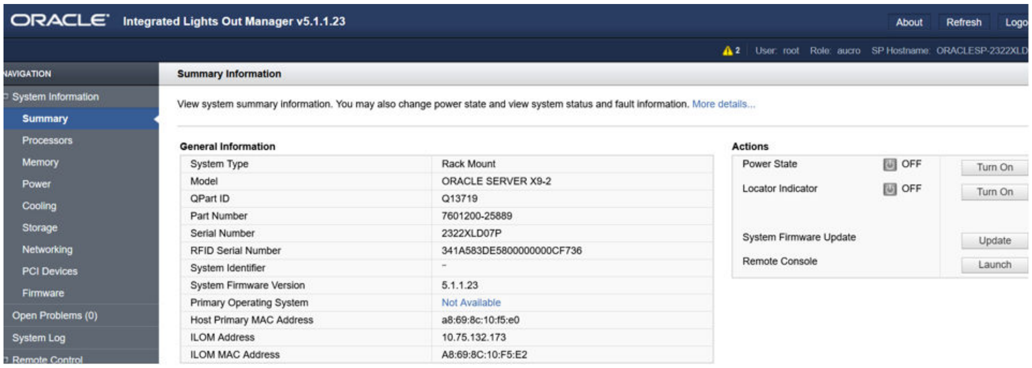
Description	Status
Auto power-on host on boot (enabling this policy disables Set host power to last power state policy)	Disabled
Set host power to last power state on boot (enabling this policy disables Auto power-on host policy)	Enabled
Set to delay host power on	Disabled
Set enhanced PCIe cooling mode policy	Disabled
Map out DIMMs with CE faults	Disabled
Immediately reset the host to map out DIMMs with excessive CE faults	Disabled
Immediately shutdown the host to clear persistent prochot	Disabled
Disable the external Host power button	Disabled

3. To reboot the server for BIOS Config, do the following:

   a. **Turn off** the power:

      Go to `iLOM/System information`

Figure 2-3 Turn off



Summary Information

View system summary information. You may also change power state and view system status and fault information. More details...

General Information

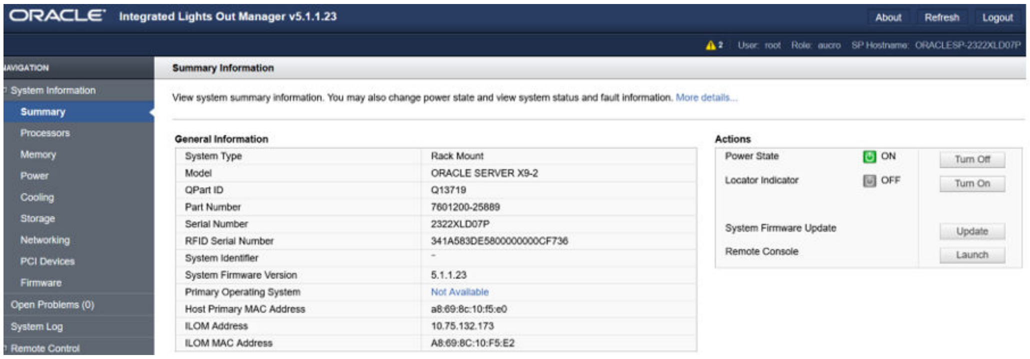
System Type	Rack Mount
Model	ORACLE SERVER X9-2
QPart ID	Q13719
Part Number	7601200-25889
Serial Number	2322XLD07P
RFID Serial Number	341A583DE5800000000CF736
System Identifier	-
System Firmware Version	5.1.1.23
Primary Operating System	Not Available
Host Primary MAC Address	a8:69:8c:10:f5:e0
ILOM Address	10.75.132.173
ILOM MAC Address	A8:69:8C:10:F5:E2

Actions

Power State	OFF	Turn On
Locator Indicator	OFF	Turn On
System Firmware Update		Update
Remote Console		Launch

b. Wait until the power turns off, and then Turn it on.

Figure 2-4 Turn on



Summary Information

View system summary information. You may also change power state and view system status and fault information. More details...

General Information

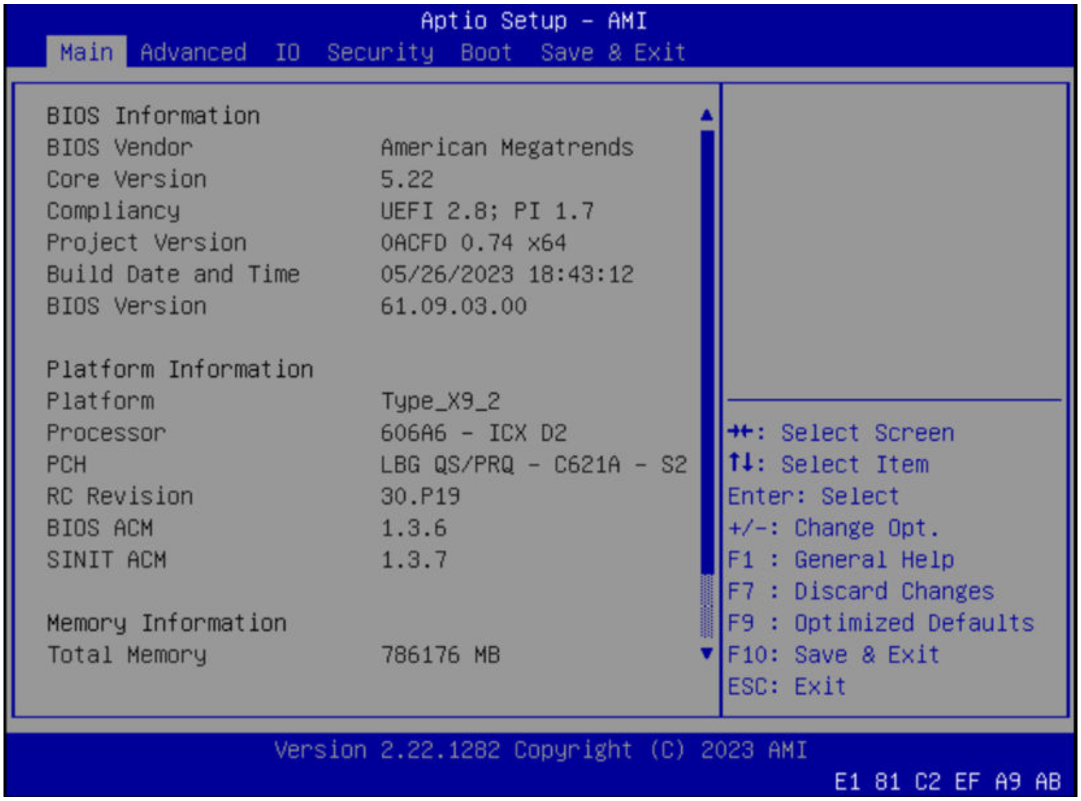
System Type	Rack Mount
Model	ORACLE SERVER X9-2
QPart ID	Q13719
Part Number	7601200-25889
Serial Number	2322XLD07P
RFID Serial Number	341A583DE5800000000CF736
System Identifier	-
System Firmware Version	5.1.1.23
Primary Operating System	Not Available
Host Primary MAC Address	a8:69:8c:10:f5:e0
ILOM Address	10.75.132.173
ILOM MAC Address	A8:69:8C:10:F5:E2

Actions

Power State	ON	Turn Off
Locator Indicator	OFF	Turn On
System Firmware Update		Update
Remote Console		Launch

4. To enable the BIOS setup, press **F2**.

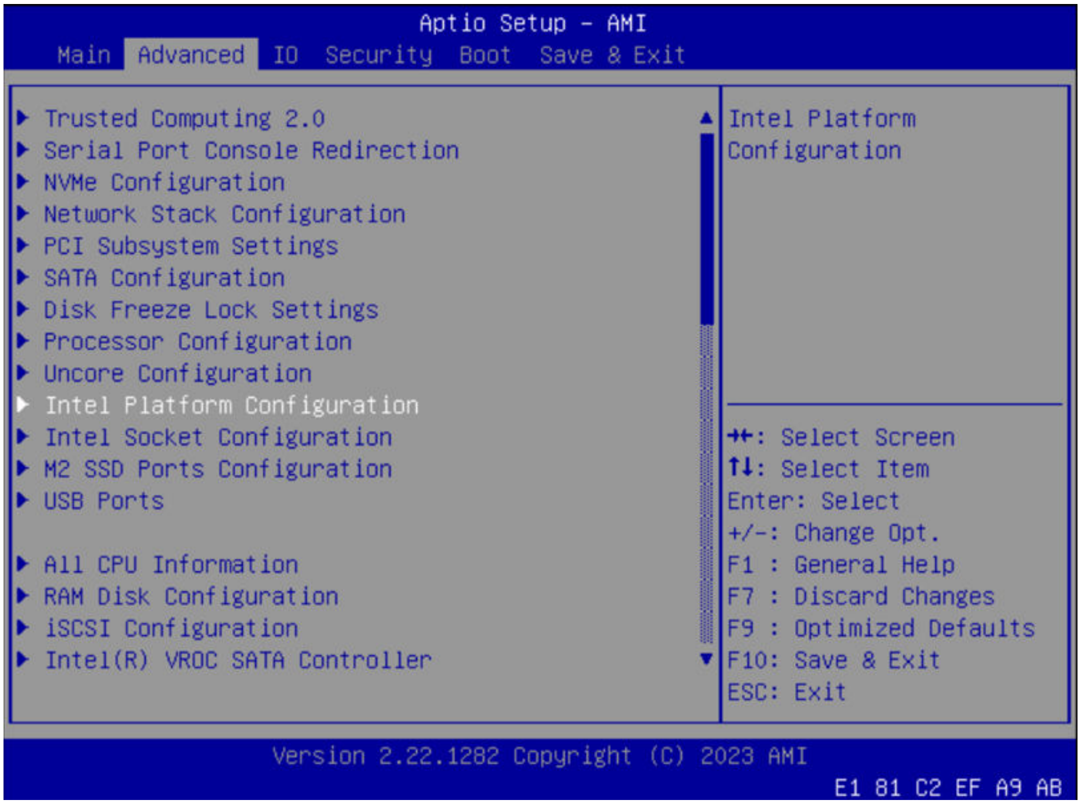
Figure 2-5 F2



```
                          Aptio Setup - AMI
  Main  Advanced  IO  Security  Boot  Save & Exit

  BIOS Information
  BIOS Vendor                 American Megatrends
  Core Version                5.22
  Compliancy                  UEFI 2.8; PI 1.7
  Project Version             0ACFD 0.74 x64
  Build Date and Time         05/26/2023 18:43:12
  BIOS Version                61.09.03.00

  Platform Information
  Platform                    Type_X9_2
  Processor                   606A6 - ICX D2          →←: Select Screen
  PCH                         LBG QS/PRQ - C621A - S2 ↑↓: Select Item
  RC Revision                 30.P19                  Enter: Select
  BIOS ACM                    1.3.6                   +/-: Change Opt.
  SINIT ACM                   1.3.7                   F1 : General Help
                                                      F7 : Discard Changes
  Memory Information                                  F9 : Optimized Defaults
  Total Memory                786176 MB               F10: Save & Exit
                                                      ESC: Exit

             Version 2.22.1282 Copyright (C) 2023 AMI
                                                E1 81 C2 EF A9 AB
```

5. After enabling the BIOS, access the BIOS Advanced tab using the arrow key.
6. Select Intel Platform Configuration using the arrow key and press **Enter**.

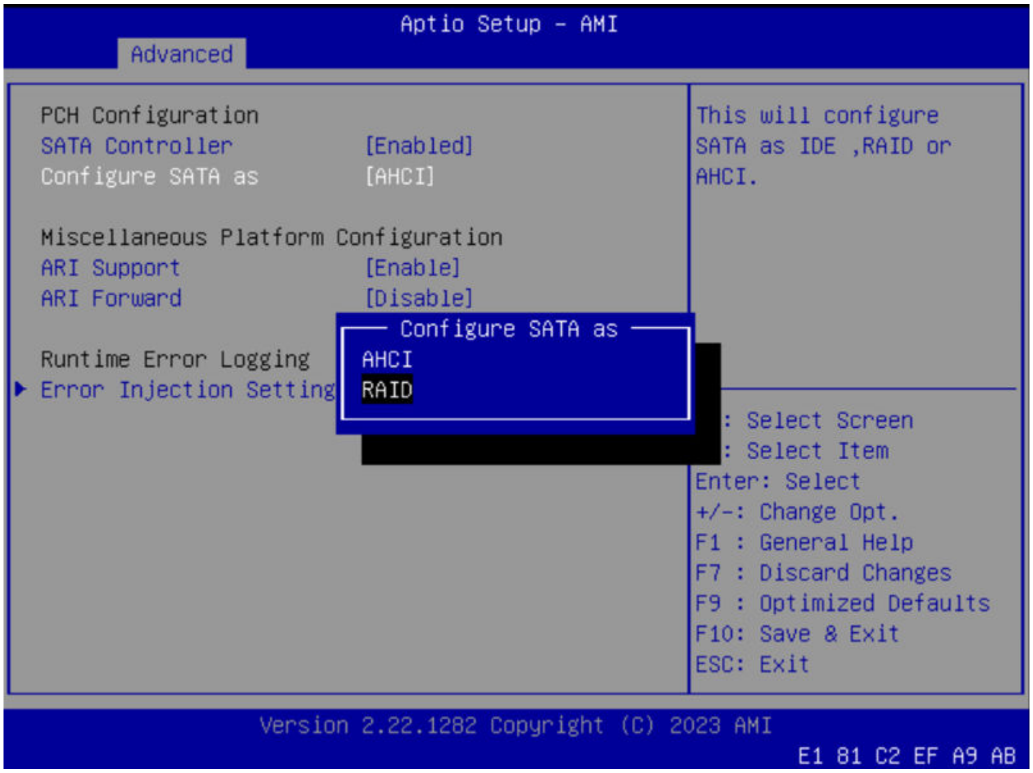
Figure 2-6 Intel platform configuration



```
                         Aptio Setup - AMI
   Main  Advanced  IO  Security  Boot  Save & Exit

 ▶ Trusted Computing 2.0                       ▲ Intel Platform
 ▶ Serial Port Console Redirection               Configuration
 ▶ NVMe Configuration
 ▶ Network Stack Configuration
 ▶ PCI Subsystem Settings
 ▶ SATA Configuration
 ▶ Disk Freeze Lock Settings
 ▶ Processor Configuration
 ▶ Uncore Configuration
 ▶ Intel Platform Configuration
 ▶ Intel Socket Configuration                    →←: Select Screen
 ▶ M2 SSD Ports Configuration                    ↑↓: Select Item
 ▶ USB Ports                                     Enter: Select
                                                 +/-: Change Opt.
 ▶ All CPU Information                           F1 : General Help
 ▶ RAM Disk Configuration                        F7 : Discard Changes
 ▶ iSCSI Configuration                           F9 : Optimized Defaults
 ▶ Intel(R) VROC SATA Controller               ▼ F10: Save & Exit
                                                 ESC: Exit

              Version 2.22.1282 Copyright (C) 2023 AMI
                                                  E1 81 C2 EF A9 AB
```

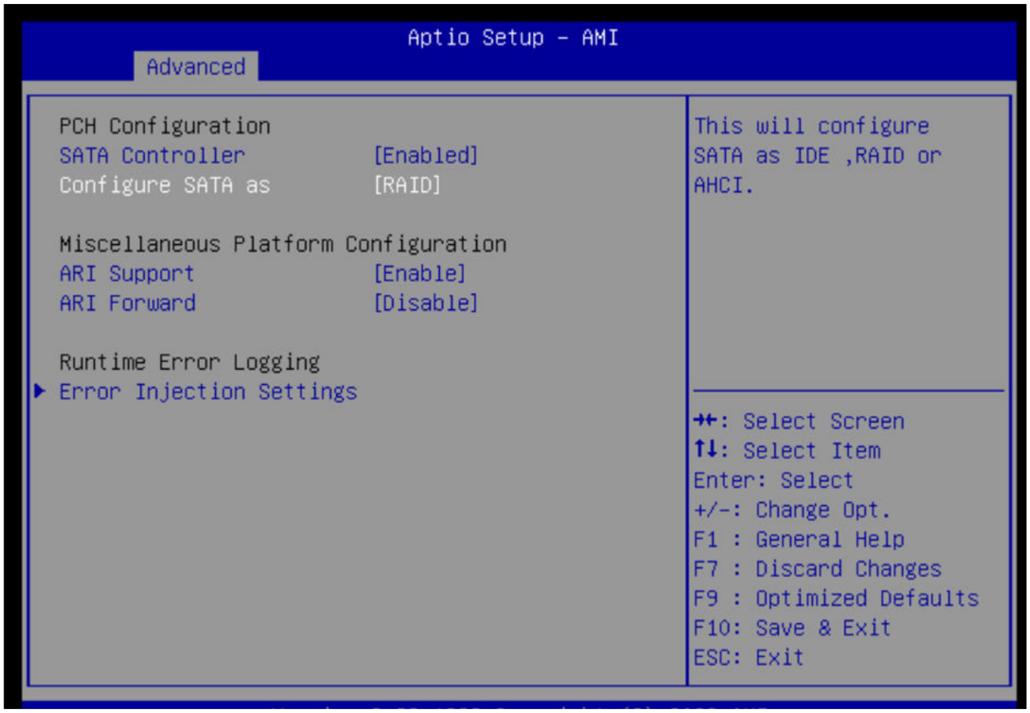
7. To verify if the SATA Controller is enabled:
   - Go to Advanced tab and verify if SATA Controller is **Enabled**
8. To verify if SATA RAID is enabled:
   - Go to Advanced tab, click on **Configure SATA as AHCI** and select **RAID**

Figure 2-7 Configure SATA



```
                         Aptio Setup - AMI
    Advanced

 PCH Configuration                                This will configure
 SATA Controller           [Enabled]              SATA as IDE ,RAID or
 Configure SATA as         [AHCI]                 AHCI.

 Miscellaneous Platform Configuration
 ARI Support               [Enable]
 ARI Forward               [Disable]
                         ─ Configure SATA as ─
 Runtime Error Logging    AHCI
▶ Error Injection Setting RAID
                                                  : Select Screen
                                                  : Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1 : General Help
                                                 F7 : Discard Changes
                                                 F9 : Optimized Defaults
                                                 F10: Save & Exit
                                                 ESC: Exit

            Version 2.22.1282 Copyright (C) 2023 AMI
                                                       E1 81 C2 EF A9 AB
```

Figure 2-8 Configure SATA



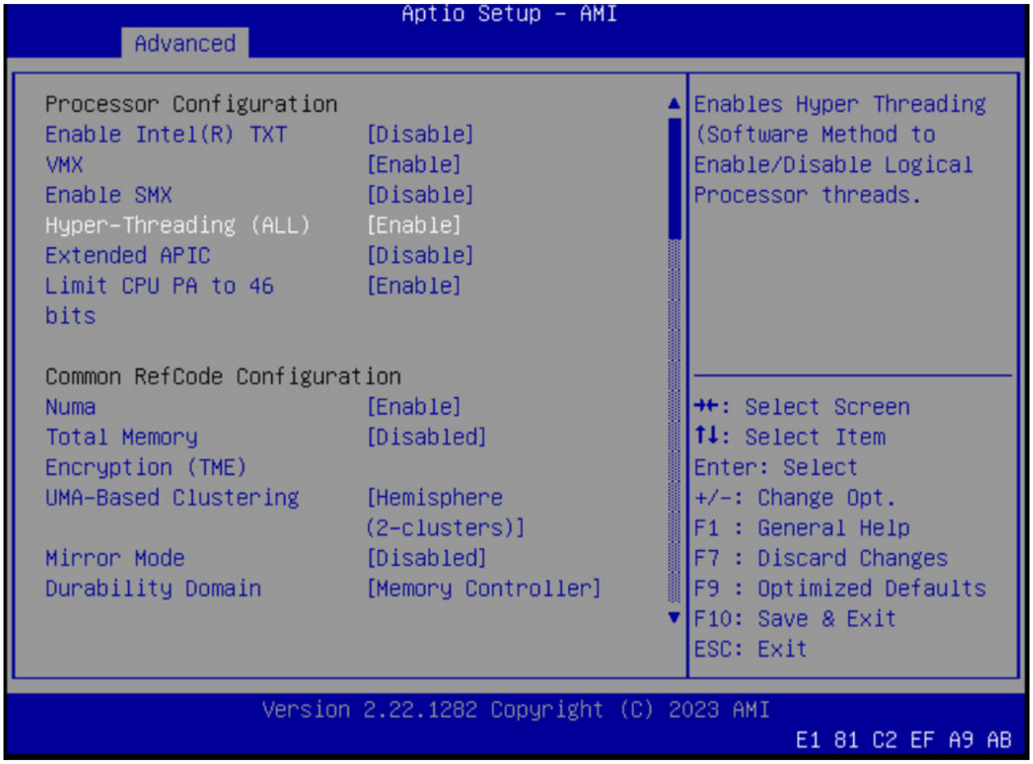
```
                         Aptio Setup - AMI
    Advanced

 PCH Configuration                                This will configure
 SATA Controller           [Enabled]              SATA as IDE ,RAID or
 Configure SATA as         [RAID]                 AHCI.

 Miscellaneous Platform Configuration
 ARI Support               [Enable]
 ARI Forward               [Disable]

 Runtime Error Logging
▶ Error Injection Settings
                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1 : General Help
                                                 F7 : Discard Changes
                                                 F9 : Optimized Defaults
                                                 F10: Save & Exit
                                                 ESC: Exit
```

> **Note**
>
> - AHCI is a hardware-level architecture that enables systems to support the use of SATA disks.
> - RAID is a logical disk structure that administrators can create at either the hardware or the software level. Administrators create RAID arrays on top of the AHCI hardware.

9. Verify if Hyper-Threading is enabled on the Advanced tab and do the following:

   - Go to `BIOS/Advanced/Intel-Socket Configuration`

Figure 2-9 Intel socket configuration

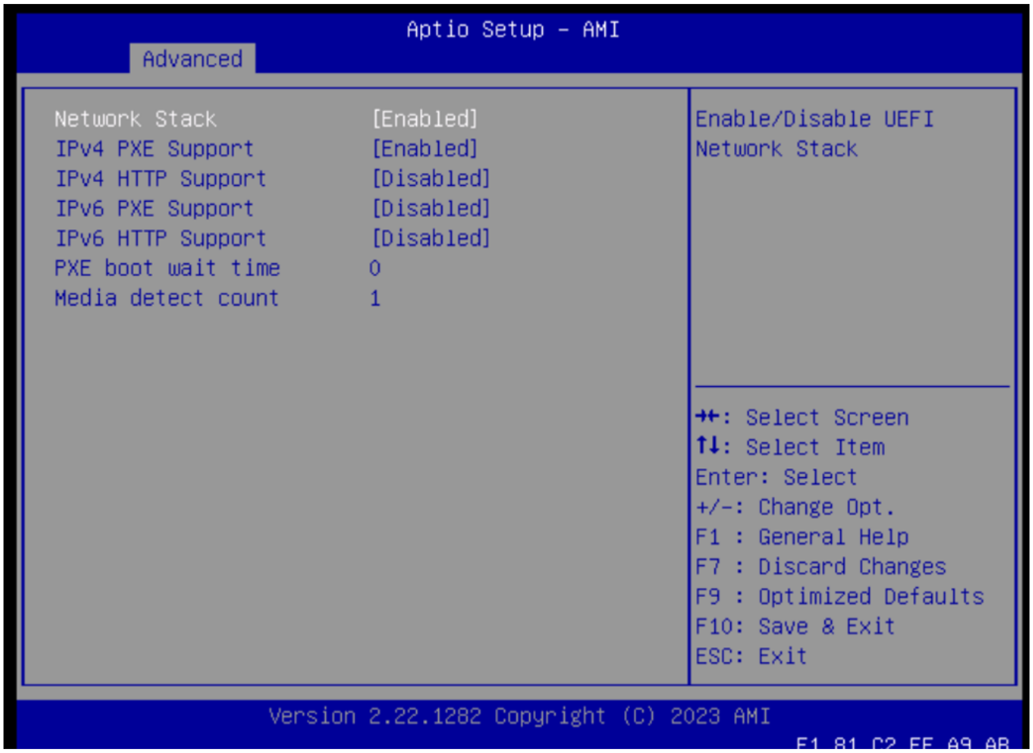


```
                         Aptio Setup - AMI
        Advanced

 Processor Configuration                    ▲ Enables Hyper Threading
 Enable Intel(R) TXT         [Disable]        (Software Method to
 VMX                         [Enable]         Enable/Disable Logical
 Enable SMX                  [Disable]        Processor threads.
 Hyper-Threading (ALL)       [Enable]
 Extended APIC               [Disable]
 Limit CPU PA to 46          [Enable]
 bits

 Common RefCode Configuration
 Numa                        [Enable]         →←: Select Screen
 Total Memory                [Disabled]       ↑↓: Select Item
 Encryption (TME)                             Enter: Select
 UMA-Based Clustering        [Hemisphere      +/-: Change Opt.
                             (2-clusters)]    F1 : General Help
 Mirror Mode                 [Disabled]       F7 : Discard Changes
 Durability Domain           [Memory Controller]  F9 : Optimized Defaults
                                            ▼ F10: Save & Exit
                                              ESC: Exit

           Version 2.22.1282 Copyright (C) 2023 AMI
                                                    E1 81 C2 EF A9 AB
```

10. Verify if Network Stack Configuration is enabled on the Advanced tab and do the following:

    - Go to `BIOS/Advanced/Network Stack Configuration`

Figure 2-10 Network stack configuration

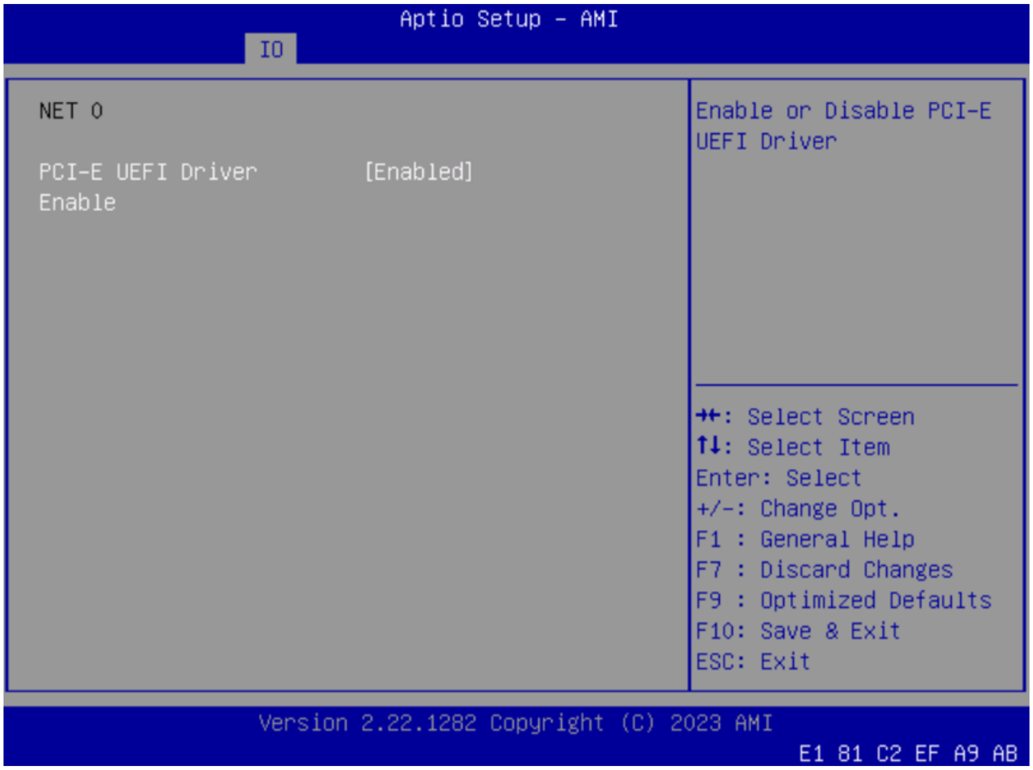


```
                         Aptio Setup - AMI
        Advanced

  Network Stack               [Enabled]          Enable/Disable UEFI
  IPv4 PXE Support            [Enabled]          Network Stack
  IPv4 HTTP Support           [Disabled]
  IPv6 PXE Support            [Disabled]
  IPv6 HTTP Support           [Disabled]
  PXE boot wait time          0
  Media detect count          1

                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1 : General Help
                                                 F7 : Discard Changes
                                                 F9 : Optimized Defaults
                                                 F10: Save & Exit
                                                 ESC: Exit

            Version 2.22.1282 Copyright (C) 2023 AMI
                                                      E1 81 C2 EF A9 AB
```

11. Verify if NET 0 is enabled on IO and do the following:

    - Go to `IO/Internal Devices /NET0/NIC0`

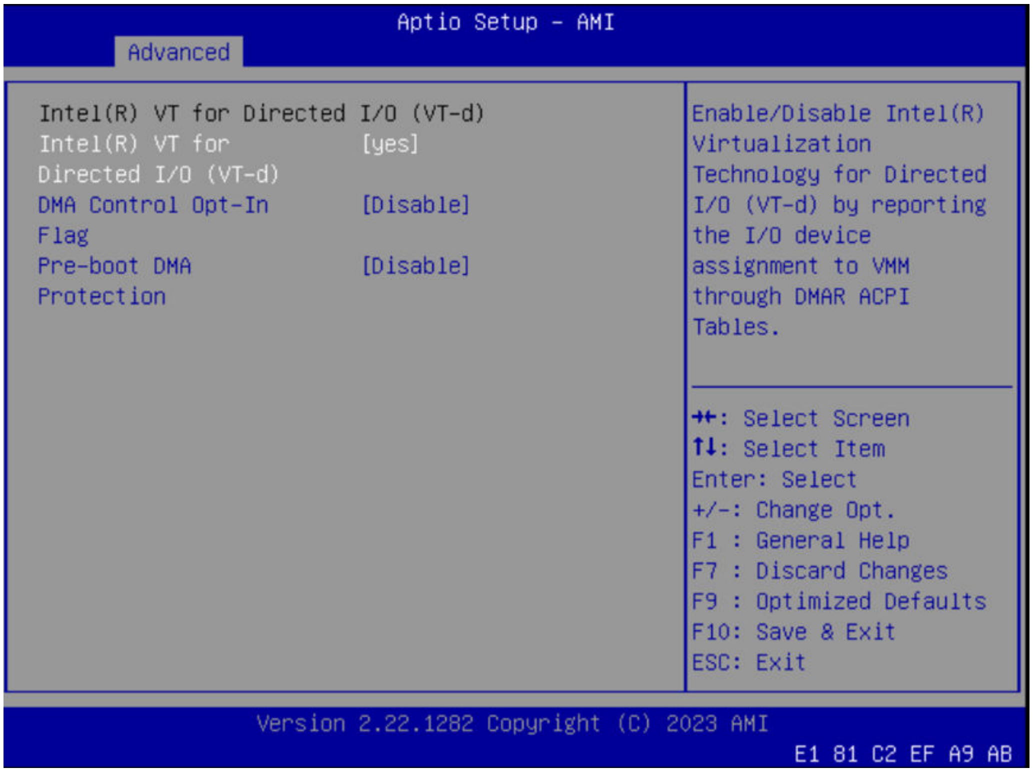
Figure 2-11 Net0



```
                         Aptio Setup - AMI
              IO

  NET 0                                          Enable or Disable PCI-E
                                                 UEFI Driver
  PCI-E UEFI Driver           [Enabled]
  Enable

                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1 : General Help
                                                 F7 : Discard Changes
                                                 F9 : Optimized Defaults
                                                 F10: Save & Exit
                                                 ESC: Exit

            Version 2.22.1282 Copyright (C) 2023 AMI
                                                      E1 81 C2 EF A9 AB
```

12. Verify if VT-d is enabled on the Advanced tab and do the following:
    - Go to `Advanced/Intel Socket Configuration/IIO Configuration-VT-d`.

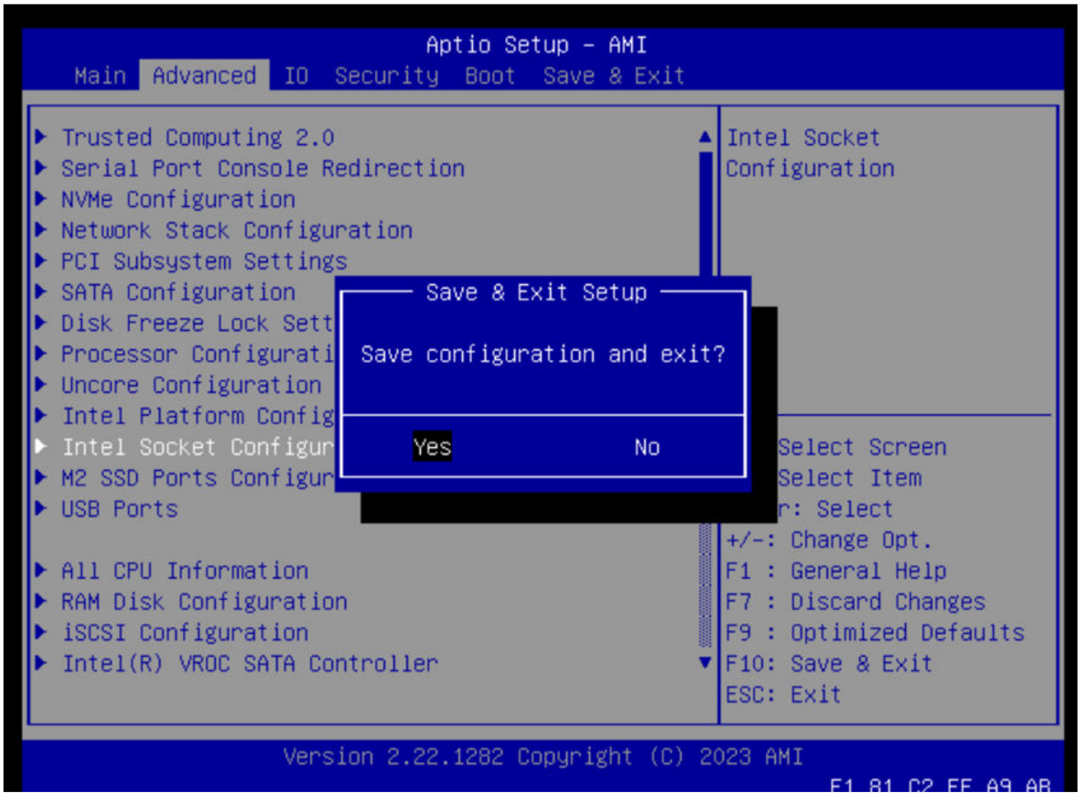
Figure 2-12 Verify Vt-d



```
Aptio Setup - AMI
Advanced

Intel(R) VT for Directed I/O (VT-d)
Intel(R) VT for             [yes]
Directed I/O (VT-d)
DMA Control Opt-In          [Disable]
Flag
Pre-boot DMA                [Disable]
Protection

Enable/Disable Intel(R)
Virtualization
Technology for Directed
I/O (VT-d) by reporting
the I/O device
assignment to VMM
through DMAR ACPI
Tables.

→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1 : General Help
F7 : Discard Changes
F9 : Optimized Defaults
F10: Save & Exit
ESC: Exit

Version 2.22.1282 Copyright (C) 2023 AMI
E1 81 C2 EF A9 AB
```

13. The server continues the boot process.
14. To save and exit, press **F10**

Figure 2-13 save and exit



Save configuration and exit?

This process concludes the Hardware Configuration verification.

2.4 Installing OL8.8 and KVM

Perform the following procedure to install Oracle Linux 8.8 OS with HTTP or USB media:

> **Note**
>
> - If you're using a hardware in a remote lab, install Linux remotely on a Windows computer. Ensure that remote Windows machine has the OL 8.8 ISO locally located.
> - The installation process is specific to Oracle Linux OS installations.
> - The Oracle Linux 8.8 release is utilized and validated for the Oracle Linux OS.
> - The snapshot used for this procedure has been taken from ORACLE SERVER X9-2 RMS.
> - This procedure can be executed on any flavor of RMS that require install on OL8.8 and KVM.

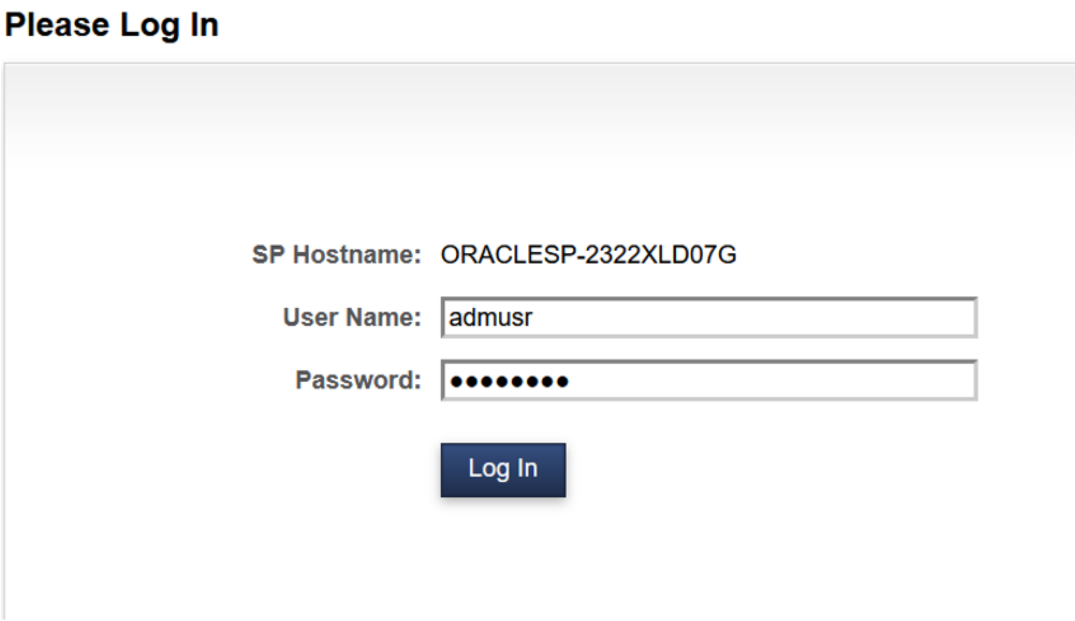
Each respective infrastructure must be operational.

Check in every step after completion.

> **Note**
>
> For any assistance, see My Oracle Support (MOS).

1. Log in to iLOM as **admusr** using the following URL: `https://<Ipv6 ILOM IP address>`.

   Figure 2-14   Log in to iLOM

   Please Log In

   SP Hostname: ORACLESP-2322XLD07G

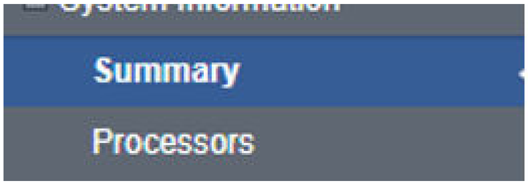
   User Name: admusr

   Password: ••••••••

2. To launch the remote console, do the following:

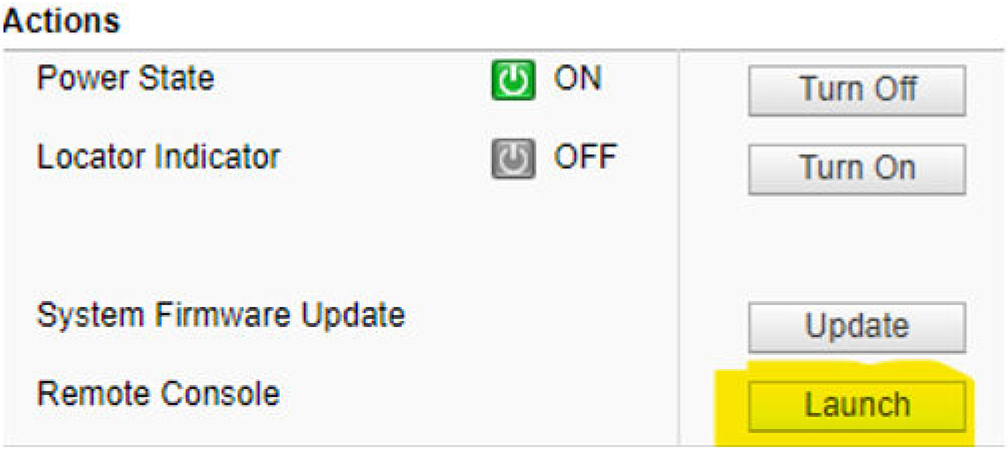
   a. Go to **Navigation** and select **Summary**.

   Figure 2-15   Summary

   b. Click **Launch** that is next to the remote console and click **Continue** on the JAVA security warning pop-up.

Figure 2-16   Launch



Actions

Power State	ON	Turn Off
Locator Indicator	OFF	Turn On
System Firmware Update		Update
Remote Console		Launch

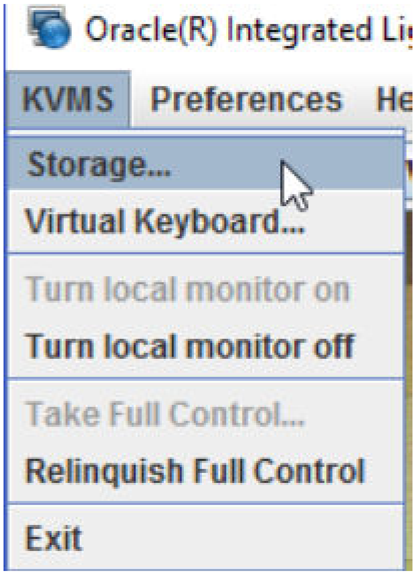
3. To install OL 8.8 image through Local USB media

> **Note**
>
> To install OL8.8, if requires HTTP server to start the media. Please skip this step and proceed with Step 4

a. On the ILOM Console, from the **KVMS** menu, select the **Storage** option.

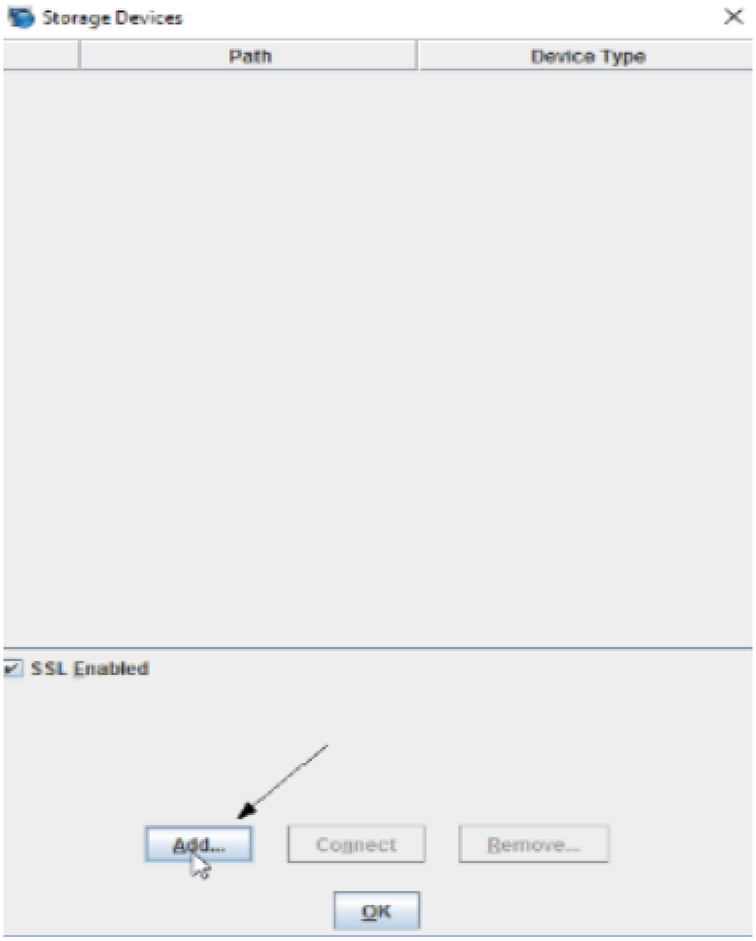
   A window entitled Storage Device will open.

Figure 2-17   Storage



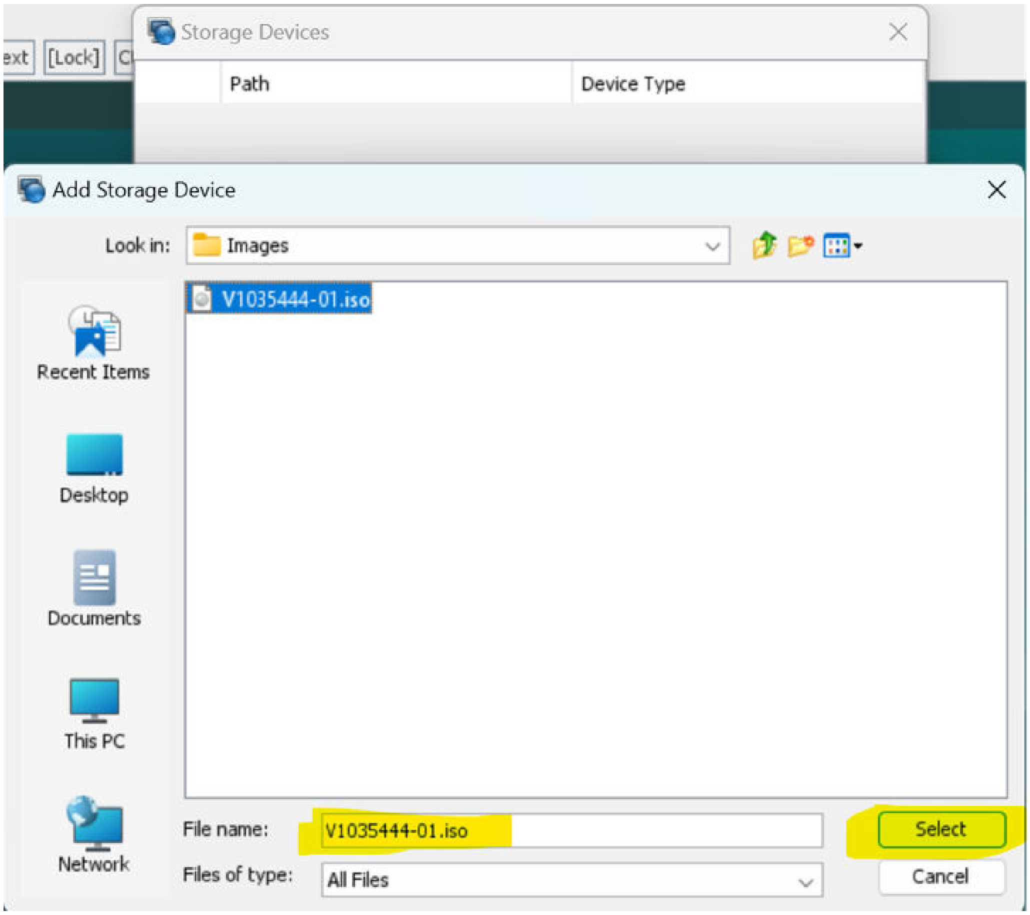
b. Click **Add** and navigate to the location of the **ISO** on the local workstation.

Figure 2-18 Storage device



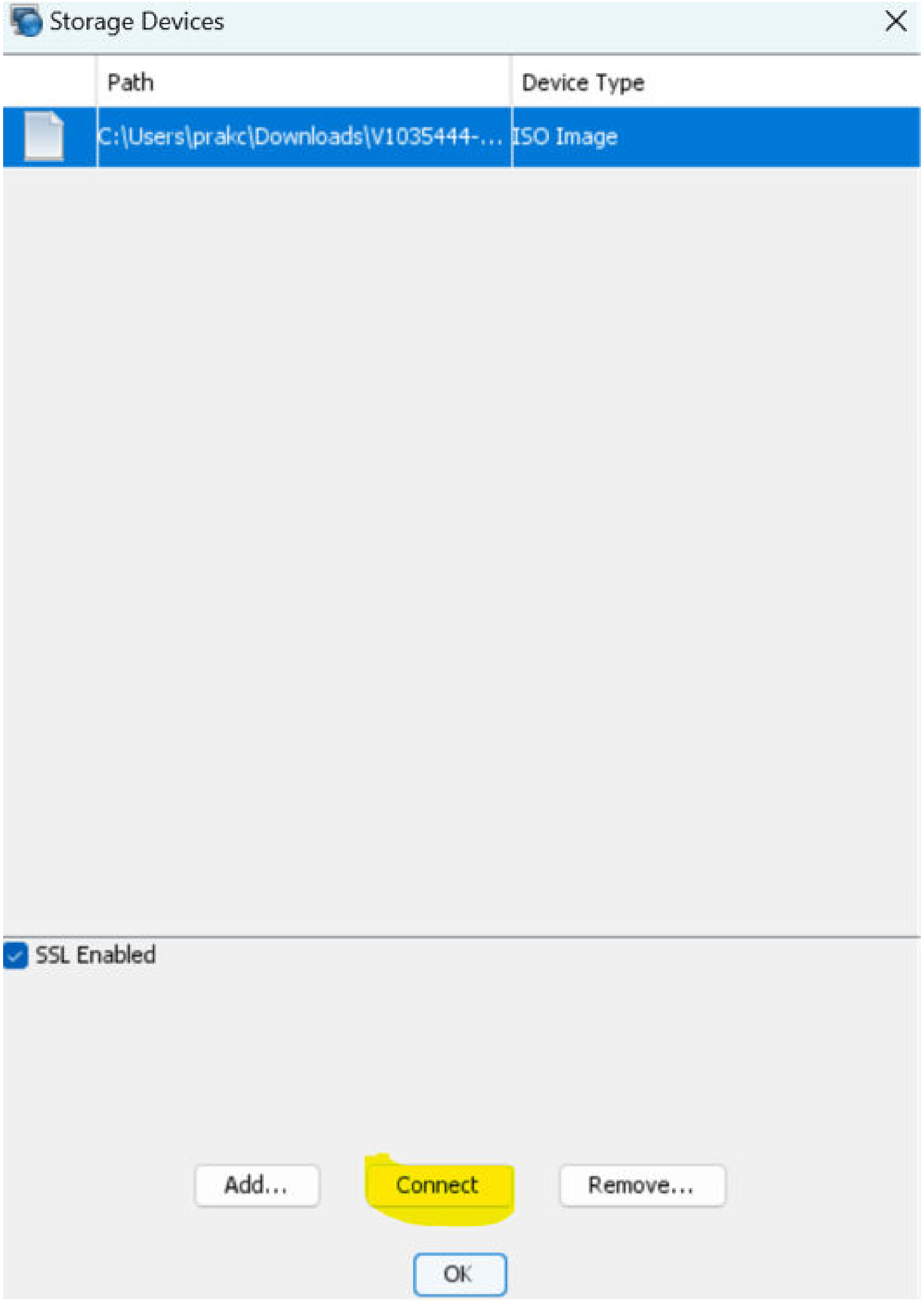
c. Select the **ISO** and click **Select**.

Figure 2-19   Select ISO



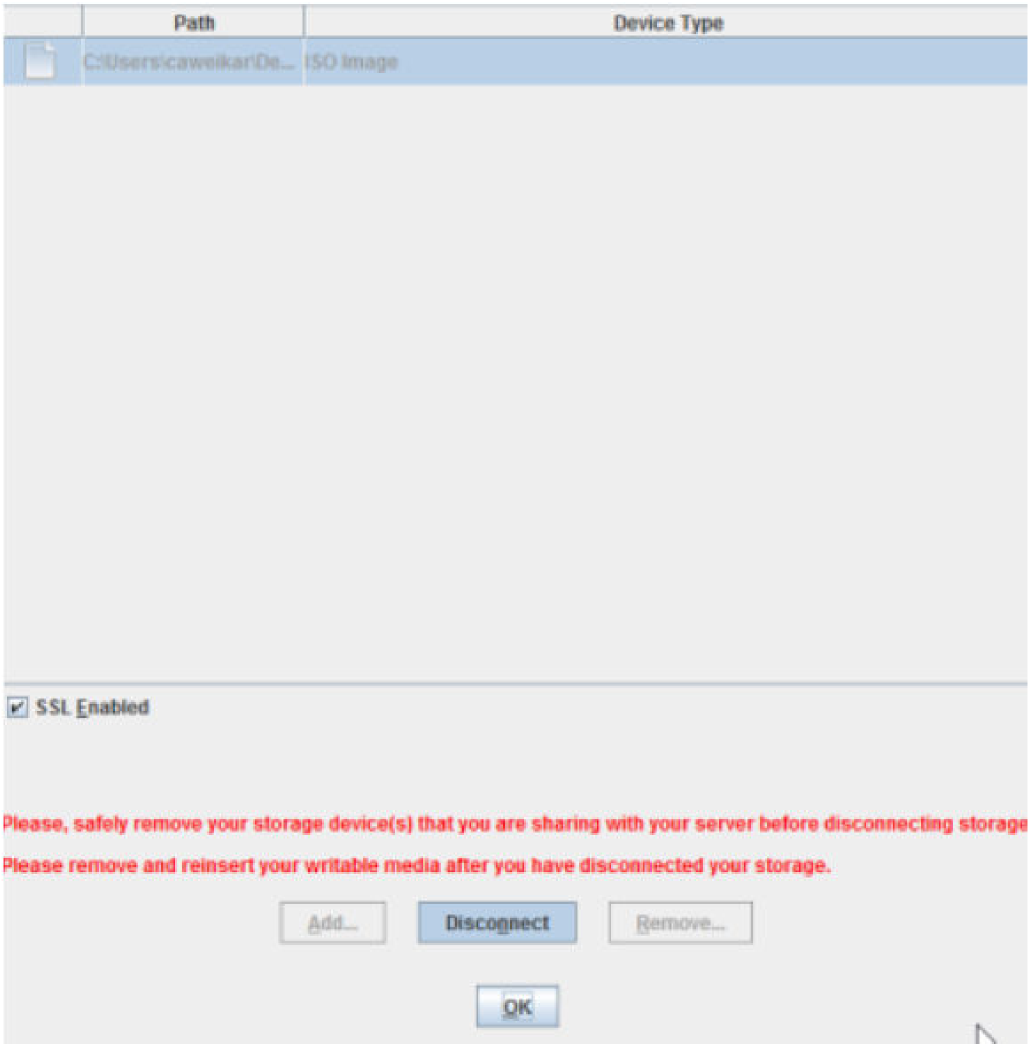
d. The ISO file will now be included in the list of available storage devices. Select it in the Storage Devices window and then click **Connect**.

Figure 2-20 Connect



e. Click **OK** to confirm and close the window.

Figure 2-21 Click OK



	Path	Device Type
	C:\Users\caweikar\De...	ISO Image

☑ SSL Enabled

Please, safely remove your storage device(s) that you are sharing with your server before disconnecting storage

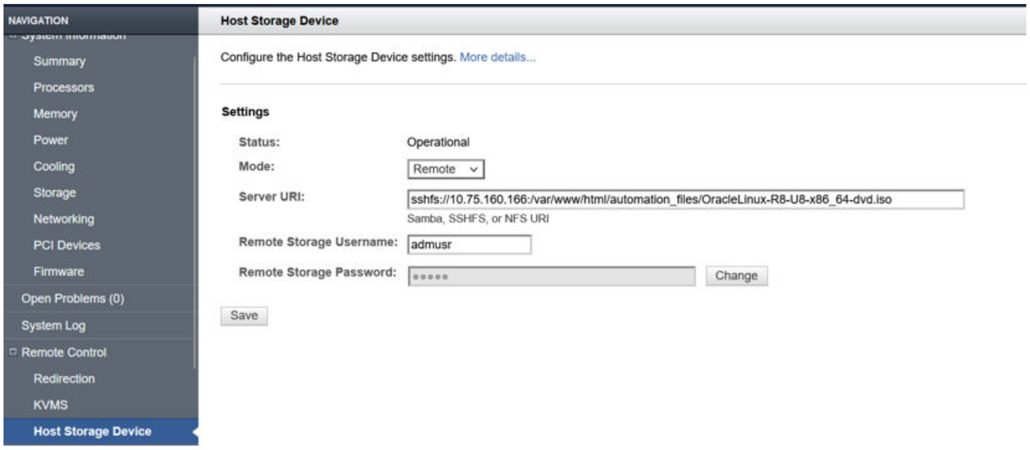
Please remove and reinsert your writable media after you have disconnected your storage.

4. Install OL 8.8 image through HTTP server.

> **Note**
>
> To install OL8.8, if requires local USB to start the media as mentioned in step 3. Please skip this step and proceed with Step 5

- Navigate to `Remote Control/Host Storage Device` to place the OL 8.8 iso image on the existing HTTP web server and connect it through Server URI in **Host Storage Device** of iLOM GUI.

Figure 2-22 Host storage device



Host Storage Device

Configure the Host Storage Device settings. More details...

Settings

Status: Operational

Mode: Remote

Server URI: sshfs://10.75.160.166:/var/www/html/automation_files/OracleLinux-R8-U8-x86_64-dvd.iso

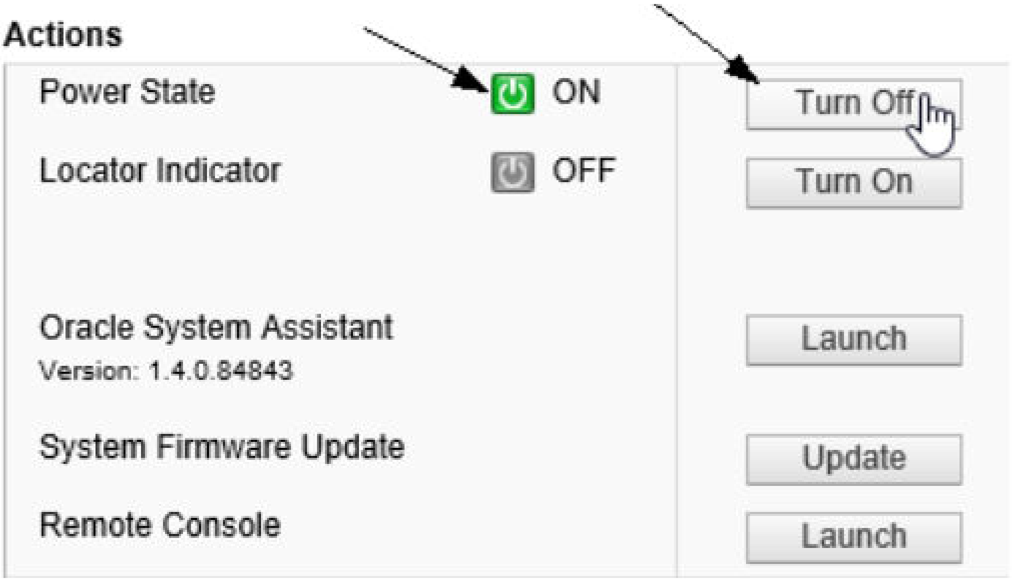
Samba, SSHFS, or NFS URI

Remote Storage Username: admusr

Remote Storage Password: •••••

5. Shut down the server
   - On the System Summary page click the **Turn Off** in the Actions Pane.

Figure 2-23 Turn off



Actions

Power State ON

Locator Indicator OFF

Oracle System Assistant
Version: 1.4.0.84843

System Firmware Update

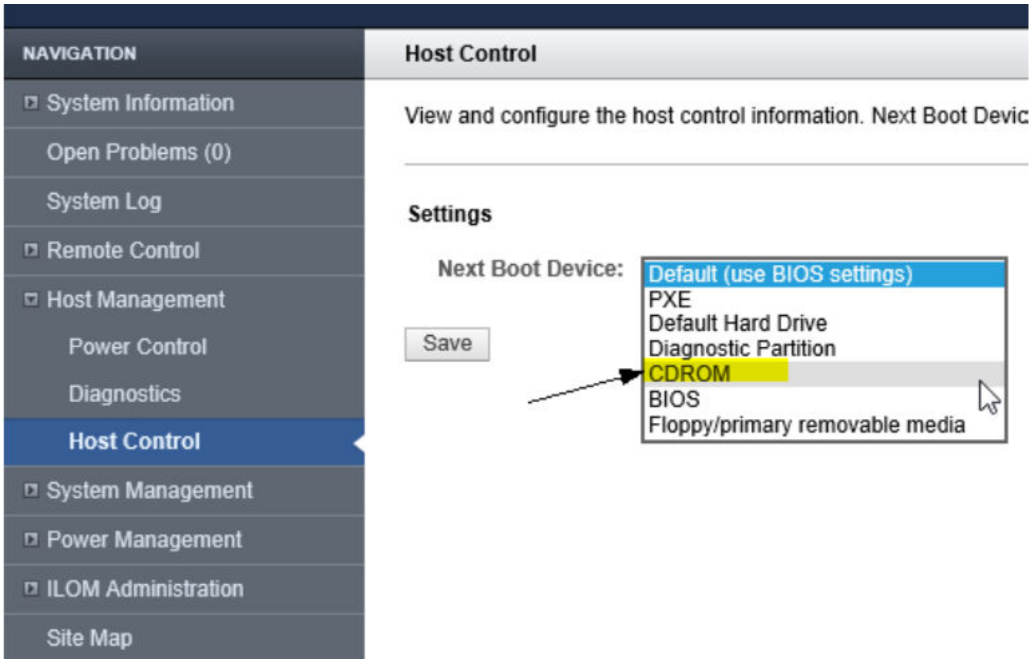
Remote Console

> ⓘ **Note**
>
> - This will shut down the operating system prior to powering off the host server. Wait for the indicator to signify that the server is powered down before proceeding to the next step.
> - If at any point the internet connection on the local workstation is lost, or the browser being used is closed, and the OSA has not yet been updated, the Oracle System Assistant Updater ISO must be remounted using the previous steps.

6. Set CDROM as the next boot device.

   - Under the Host Management tab select the **Host Control** option. From the drop-down menu for Next Boot Device, select the **CDROM** option and then click **Save**

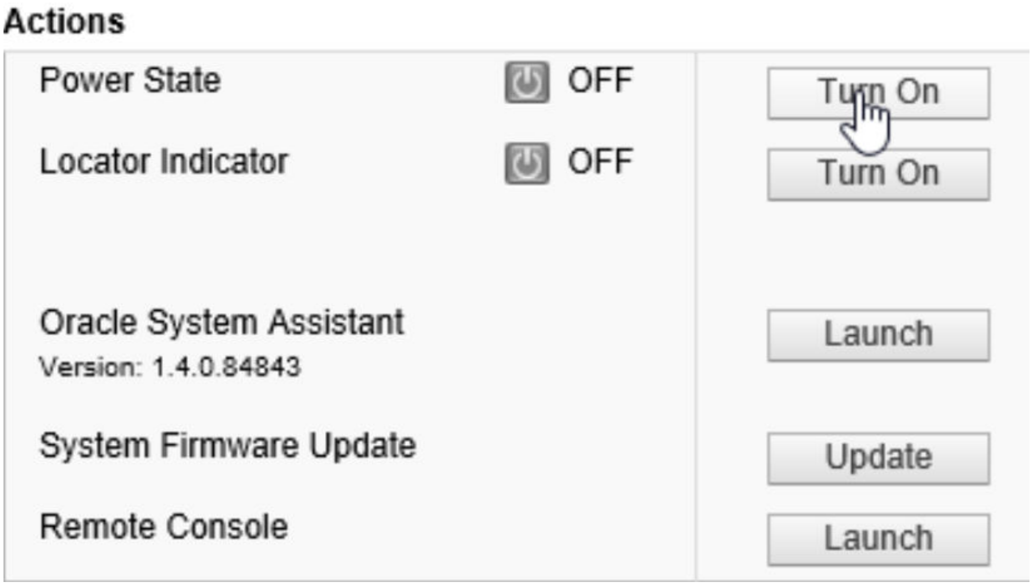
Figure 2-24 CDROM



7. **Power ON** the server

   a. On the System Summary page click the **Power State Turn On** in the **Actions Pane** to restart into the Oracle System Assistant Updater ISO.

Figure 2-25 Power on



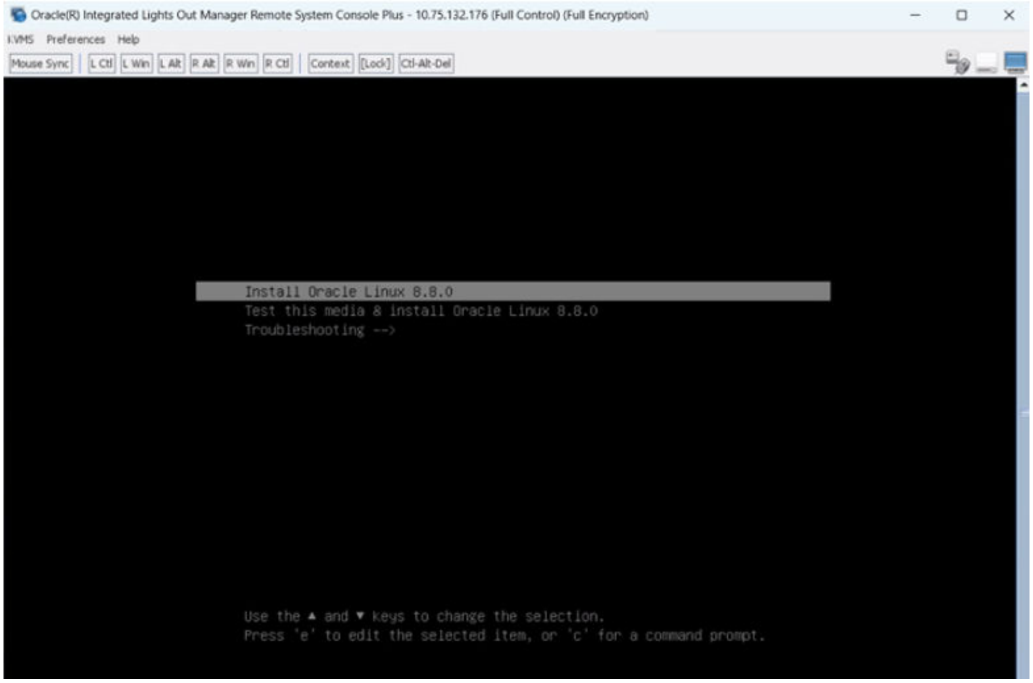
   b. Click **OK** when prompted.

8. Perform the following procedure to install **Oracle Linux OS**

   a. Navigate to the window that contains the Remote Console. If the window was closed, re-launch the Console in the **Actions** Pane. The system will restart for installation.

   b. Select **install Oracle Linux 8.8** and click **Enter**.

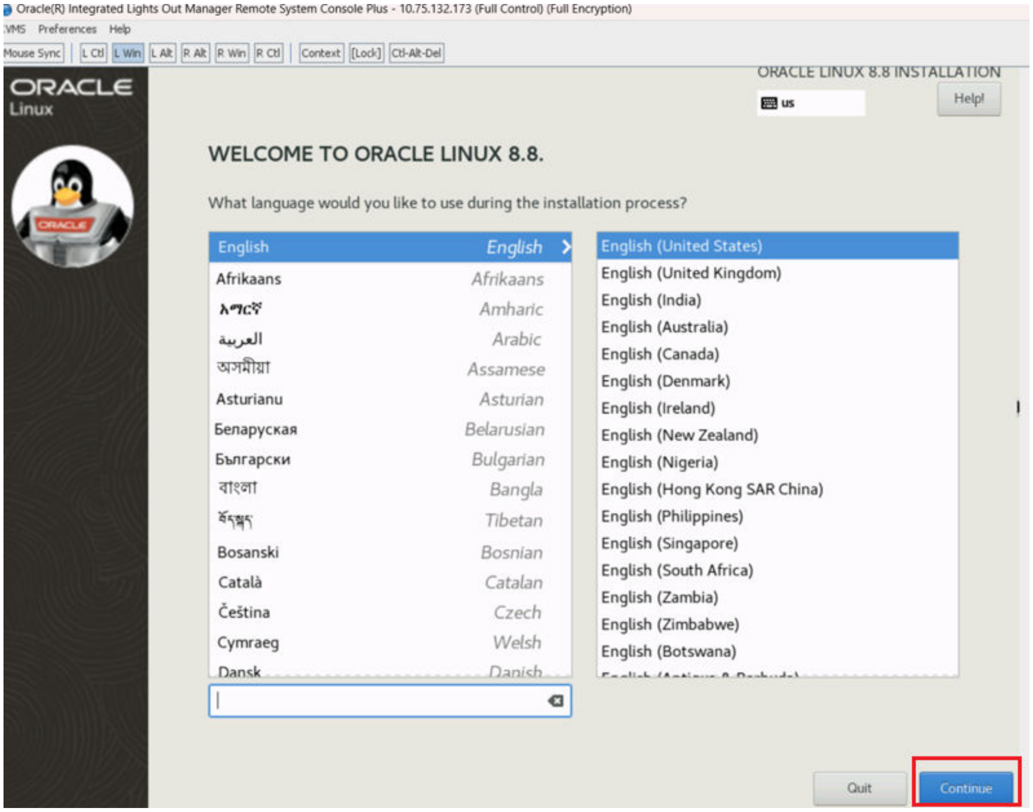
Figure 2-26 Install linux


Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.176 (Full Control) (Full Encryption)
KVMS
Preferences
Help
Mouse Sync
L Ctl
L Win
L Alt
R Alt
R Win
R Ctl
Context
Lock
Ctl-Alt-Del

```
Install Oracle Linux 8.8.0
Test this media & install Oracle Linux 8.8.0
Troubleshooting -->

Use the ▲ and ▼ keys to change the selection.
Press 'e' to edit the selected item, or 'c' for a command prompt.
```

   c. Select Language and **Continue**.

Figure 2-27 Language


Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryption)
KVMS Preferences Help
Mouse Sync | L Ctl | L Win | L Alt | R Alt | R Win | R Ctl | Context | [Lock] | Ctl-Alt-Del
ORACLE Linux
ORACLE LINUX 8.8 INSTALLATION
us
Help!
Quit
Continue

WELCOME TO ORACLE LINUX 8.8.

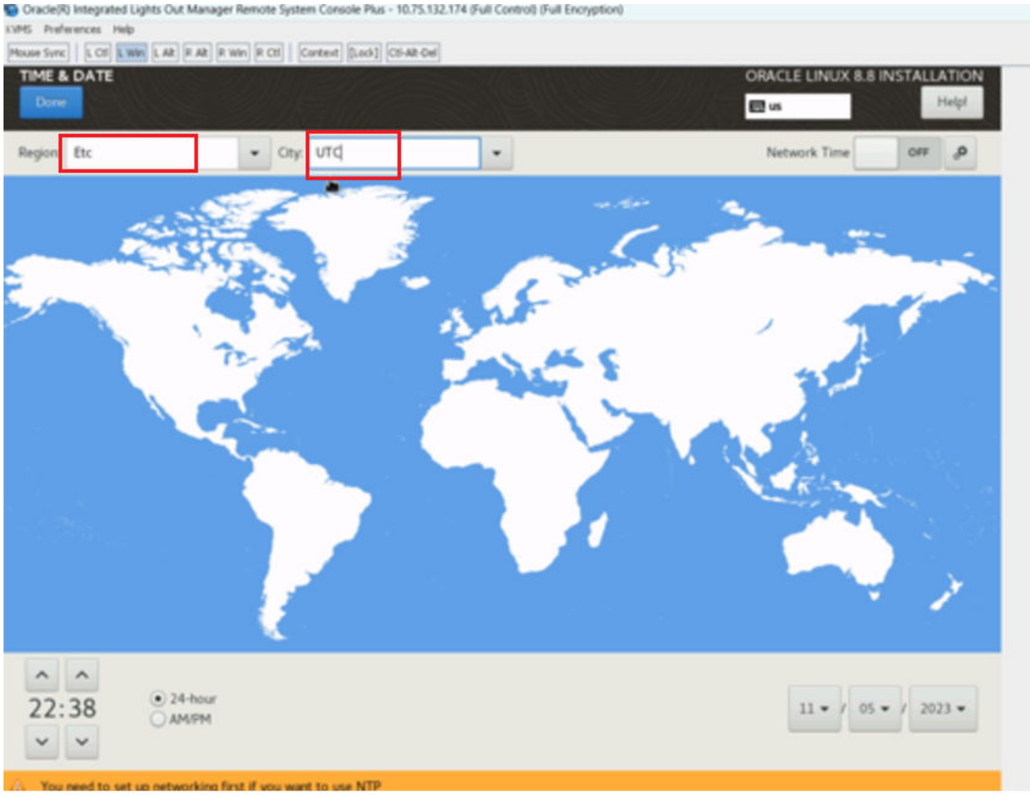
What language would you like to use during the installation process?

English	English
Afrikaans	Afrikaans
አማርኛ	Amharic
العربية	Arabic
অসমীয়া	Assamese
Asturianu	Asturian
Беларуская	Belarusian
Български	Bulgarian
বাংলা	Bangla
བོད་སྐད	Tibetan
Bosanski	Bosnian
Català	Catalan
Čeština	Czech
Cymraeg	Welsh
Dansk	Danish

- English (United States)
- English (United Kingdom)
- English (India)
- English (Australia)
- English (Canada)
- English (Denmark)
- English (Ireland)
- English (New Zealand)
- English (Nigeria)
- English (Hong Kong SAR China)
- English (Philippines)
- English (Singapore)
- English (South Africa)
- English (Zambia)
- English (Zimbabwe)
- English (Botswana)
- English (Antigua & Barbuda)

d. Select Date and Time and then select **Done**.

Figure 2-28   Date and time


Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.174 (Full Control) (Full Encryption)
KVMS
Preferences
Help
Mouse Sync
L Ctl
L Win
L Alt
R Alt
R Win
R Ctl
Context
[Lock]
Ctl-Alt-Del
TIME & DATE
Done
ORACLE LINUX 8.8 INSTALLATION
us
Help!
OFF

Region: Etc

City: UTC

Network Time: OFF

22:38

● 24-hour
○ AM/PM

11 / 05 / 2023

⚠ You need to set up networking first if you want to use NTP

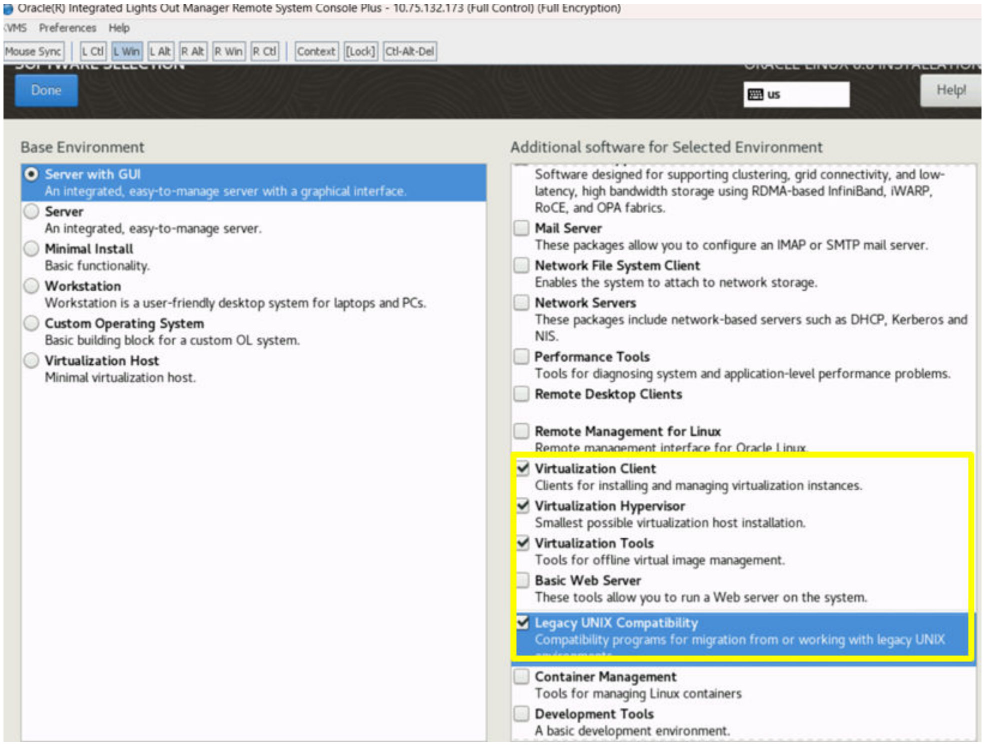
e. Select Region as **ETC** and City as **UTC**

f. Select Software selection with the following options:

   i. Basic Environment: Server with GUI

   ii. Select the following add-ons on Additional software for Selected Environment:

      - Virtualization Client
      - Virtualization Hypervisor
      - Virtualization Tools
      - Legacy UNIX Compatibility Libraries



Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryption)
KVMS Preferences Help
Mouse Sync | L Ctl | L Win | L Alt | R Alt | R Win | R Ctl | Context | [Lock] | Ctl-Alt-Del
SOFTWARE SELECTION
ORACLE LINUX 8.8 INSTALLATION
Done
us
Help!

Base Environment

- ● **Server with GUI** An integrated, easy-to-manage server with a graphical interface.
- ○ **Server** An integrated, easy-to-manage server.
- ○ **Minimal Install** Basic functionality.
- ○ **Workstation** Workstation is a user-friendly desktop system for laptops and PCs.
- ○ **Custom Operating System** Basic building block for a custom OL system.
- ○ **Virtualization Host** Minimal virtualization host.

Additional software for Selected Environment

- Software designed for supporting clustering, grid connectivity, and low-latency, high bandwidth storage using RDMA-based InfiniBand, iWARP, RoCE, and OPA fabrics.
- □ **Mail Server** These packages allow you to configure an IMAP or SMTP mail server.
- □ **Network File System Client** Enables the system to attach to network storage.
- □ **Network Servers** These packages include network-based servers such as DHCP, Kerberos and NIS.
- □ **Performance Tools** Tools for diagnosing system and application-level performance problems.
- □ **Remote Desktop Clients**
- □ **Remote Management for Linux** Remote management interface for Oracle Linux
- ☑ **Virtualization Client** Clients for installing and managing virtualization instances.
- ☑ **Virtualization Hypervisor** Smallest possible virtualization host installation.
- ☑ **Virtualization Tools** Tools for offline virtual image management.
- □ **Basic Web Server** These tools allow you to run a Web server on the system.
- ☑ **Legacy UNIX Compatibility** Compatibility programs for migration from or working with legacy UNIX environments.
- □ **Container Management** Tools for managing Linux containers
- □ **Development Tools** A basic development environment.

g. Confirm and click **Done**.

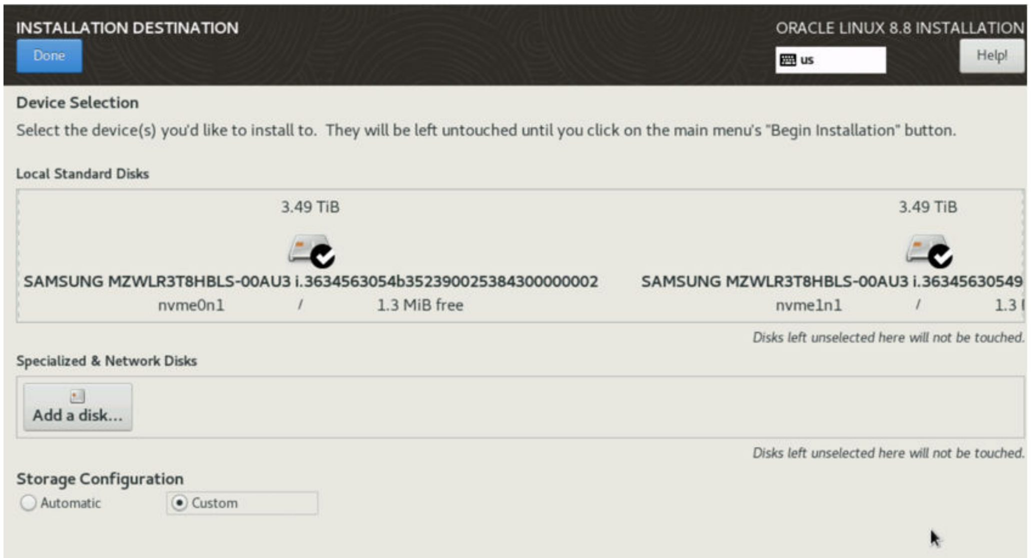
h. Select Installation Destination

i. Select 2 hard drives to be installed.

j. From **Other Storage Options**, ensure **Custom configure partitioning** is selected.

k. Click **Done**.

Figure 2-29 Click done



Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

3.49 TiB	3.49 TiB
SAMSUNG MZWLR3T8HBLS-00AU3 i.3634563054b352390025384300000002	SAMSUNG MZWLR3T8HBLS-00AU3 i.36345630549
nvme0n1 / 1.3 MiB free	nvme1n1 / 1.3

Disks left unselected here will not be touched.

Specialized & Network Disks

Add a disk...

Disks left unselected here will not be touched.

Storage Configuration

○ Automatic ● Custom

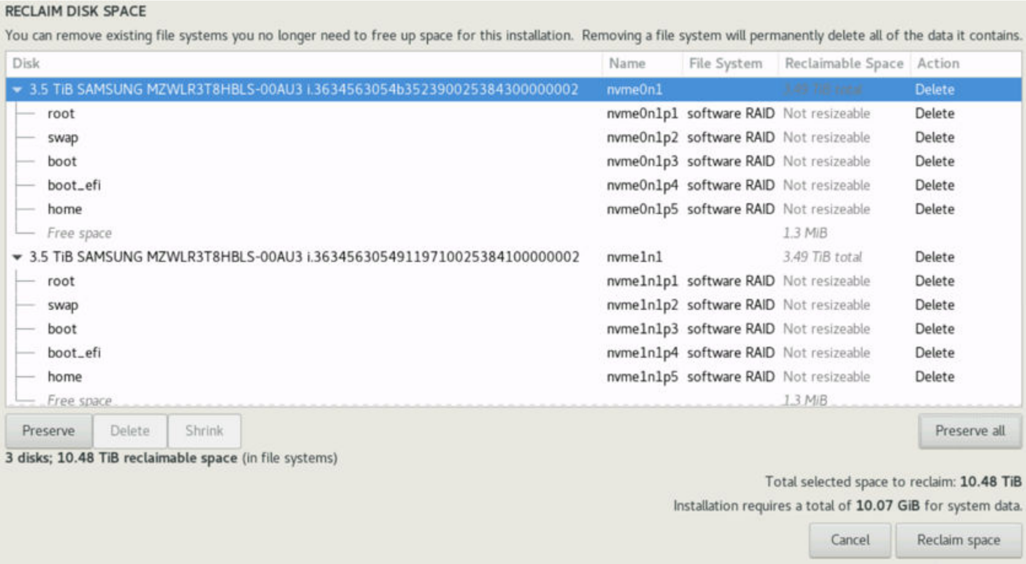
> **Note**
>
> Skip to **Step 6** if space is available for partitioning.

l. If there is not enough disk space, check if you can make additional space, on the **Other Storage Options.**

> **Note**
>
> You may need to check the box with Automatically configure partition, later select Custom Configure.

m. When you click **Done**, the following screen will allow you to **Delete all**, then **Reclaim space**

Figure 2-30   Reclaim space



RECLAIM DISK SPACE

You can remove existing file systems you no longer need to free up space for this installation. Removing a file system will permanently delete all of the data it contains.

Disk	Name	File System	Reclaimable Space	Action
3.5 TiB SAMSUNG MZWLR3T8HBLS-00AU3 i.3634563054b35239002538430000002	nvme0n1		3.49 TiB total	Delete
root	nvme0n1p1	software RAID	Not resizeable	Delete
swap	nvme0n1p2	software RAID	Not resizeable	Delete
boot	nvme0n1p3	software RAID	Not resizeable	Delete
boot_efi	nvme0n1p4	software RAID	Not resizeable	Delete
home	nvme0n1p5	software RAID	Not resizeable	Delete
Free space			1.3 MiB	
3.5 TiB SAMSUNG MZWLR3T8HBLS-00AU3 i.36345630549119710025384100000002	nvme1n1		3.49 TiB total	Delete
root	nvme1n1p1	software RAID	Not resizeable	Delete
swap	nvme1n1p2	software RAID	Not resizeable	Delete
boot	nvme1n1p3	software RAID	Not resizeable	Delete
boot_efi	nvme1n1p4	software RAID	Not resizeable	Delete
home	nvme1n1p5	software RAID	Not resizeable	Delete
Free space			1.3 MiB	

3 disks; 10.48 TiB reclaimable space (in file systems)

Total selected space to reclaim: **10.48 TiB**

Installation requires a total of **10.07 GiB** for system data.

n. Click **Done** to continue.

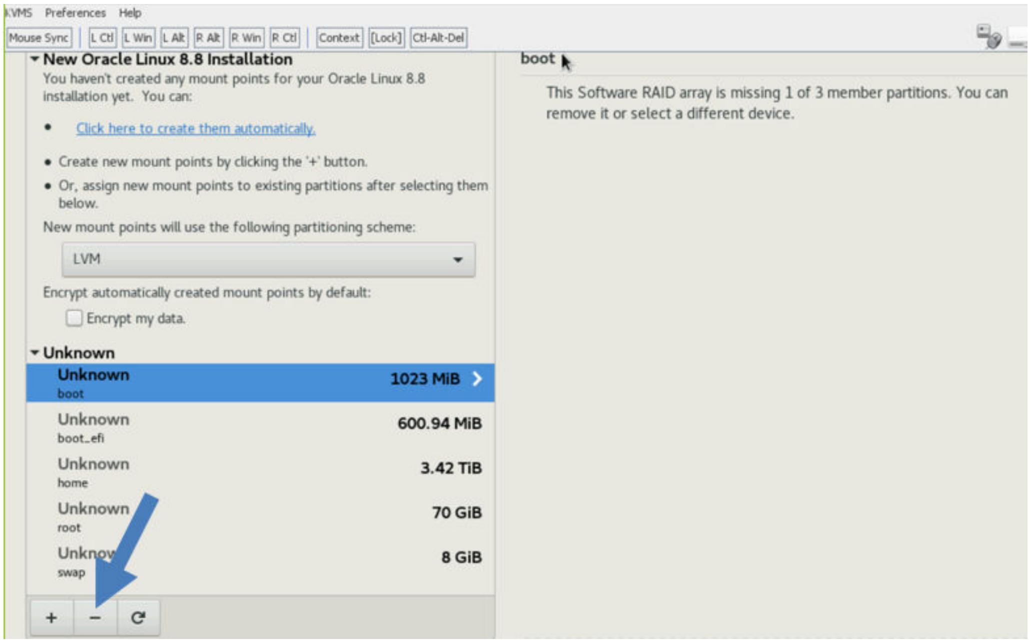
o. Again, select the **Installation Destination**.

p. From **Other Storage Options**, select **Custom configure partitioning**.

q. Remove any unknown volume by clicking on **Delete** .

> **Note**
>
> Skip this step if no unknown volume is present.

Figure 2-31   Unknown volume



▾ New Oracle Linux 8.8 Installation

You haven't created any mount points for your Oracle Linux 8.8 installation yet. You can:

- Click here to create them automatically.
- Create new mount points by clicking the '+' button.
- Or, assign new mount points to existing partitions after selecting them below.

New mount points will use the following partitioning scheme:

LVM

Encrypt automatically created mount points by default:

□ Encrypt my data.

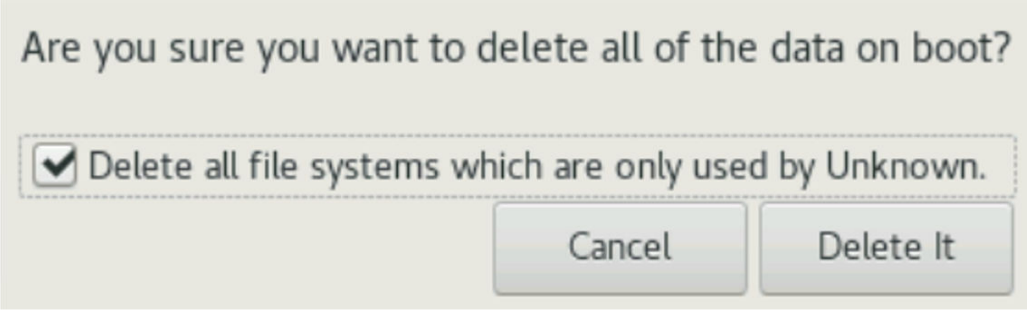
▾ Unknown

Unknown boot	1023 MiB
Unknown boot_efi	600.94 MiB
Unknown home	3.42 TiB
Unknown root	70 GiB
Unknown swap	8 GiB

boot

This Software RAID array is missing 1 of 3 member partitions. You can remove it or select a different device.

Figure 2-32   Delete



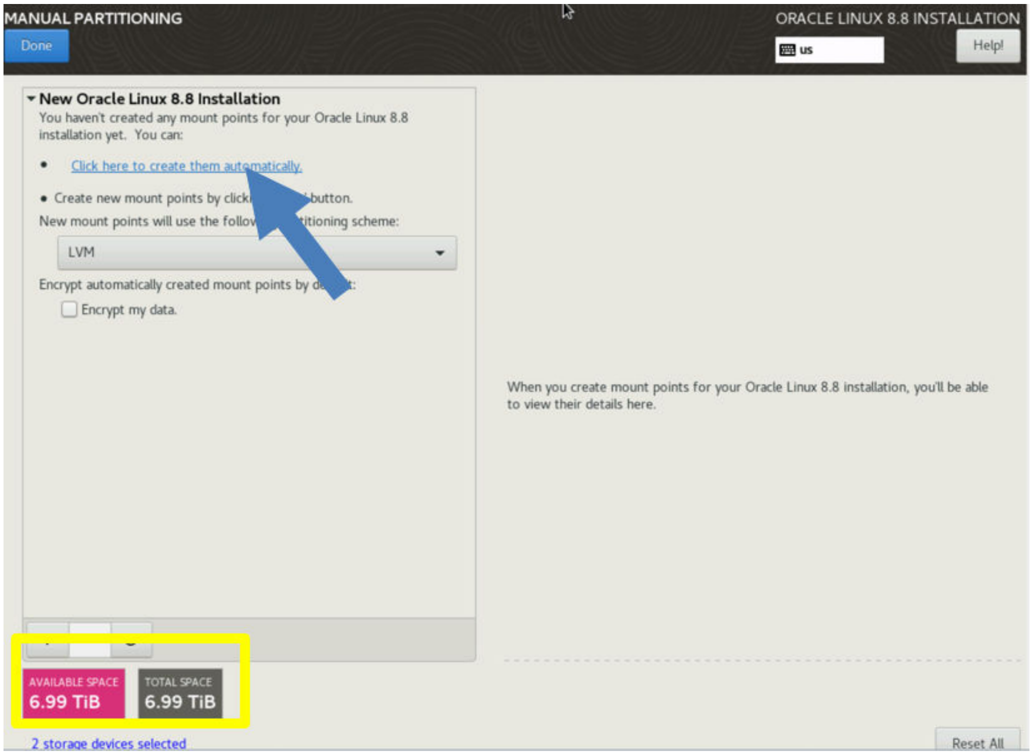
Are you sure you want to delete all of the data on boot?

☑ Delete all file systems which are only used by Unknown.

r. Ensure the Available Space = Total Space.

s. Click on **Click here to create them automatically**.

Figure 2-33 Available space



New Oracle Linux 8.8 Installation

You haven't created any mount points for your Oracle Linux 8.8 installation yet. You can:

- Click here to create them automatically.
- Create new mount points by click[...] button.

New mount points will use the follow[...]titioning scheme:

LVM

Encrypt automatically created mount points by de[...]t:

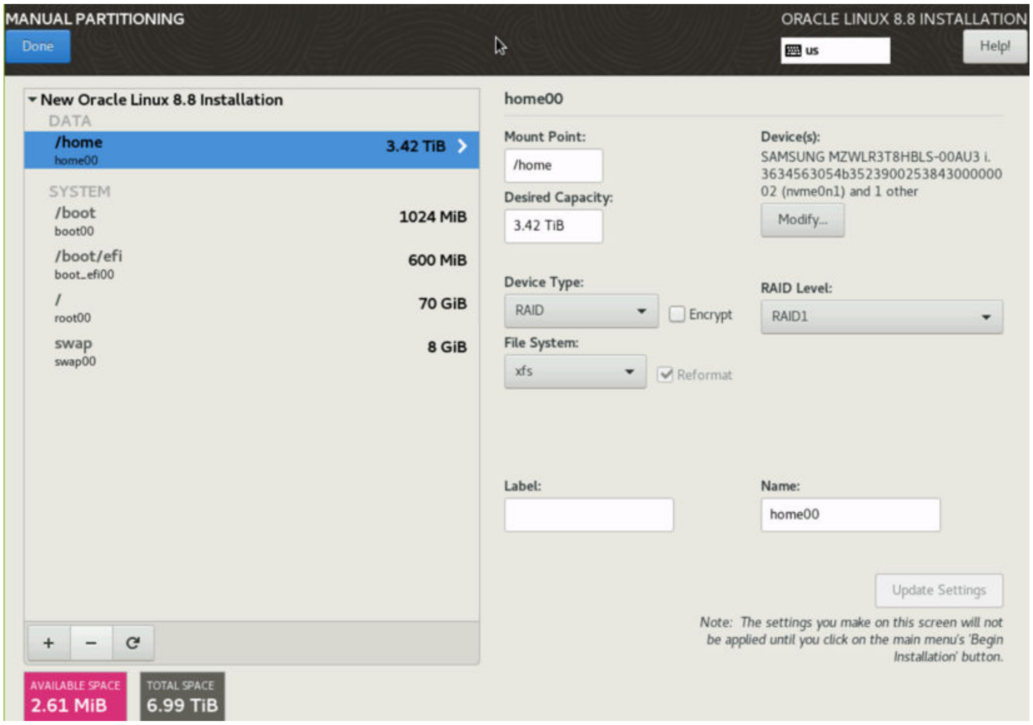
□ Encrypt my data.

When you create mount points for your Oracle Linux 8.8 installation, you'll be able to view their details here.

Table 2-3 Manual partitioning

Partition	Size	Device Type	RAID Level	Format (Syatem Default)
/	70 GiB	RAID	RAID1	ext4 or xfs
/boot	1024 MiB	RAID	RAID1	ext4 or xfs
/boot/efi	600 MiB	RAID	RAID1	efi
/home	3.4 (Remaining all) TiB	RAID	RAID1	ext4 or xfs
/swap	8 GiB	RAID	RAID1	swap

Figure 2-34 Manual partitioning boot



New Oracle Linux 8.8 Installation

DATA

/home home00	3.42 TiB

SYSTEM

/boot boot00	1024 MiB
/boot/efi boot_efi00	600 MiB
/ root00	70 GiB
swap swap00	8 GiB

AVAILABLE SPACE 2.61 MiB

TOTAL SPACE 6.99 TiB

home00

Mount Point: /home

Desired Capacity: 3.42 TiB

Device(s): SAMSUNG MZWLR3T8HBLS-00AU3 i. 3634563054b35239002538430000002 (nvme0n1) and 1 other

Modify...

Device Type: RAID □ Encrypt

RAID Level: RAID1

File System: xfs ☑ Reformat

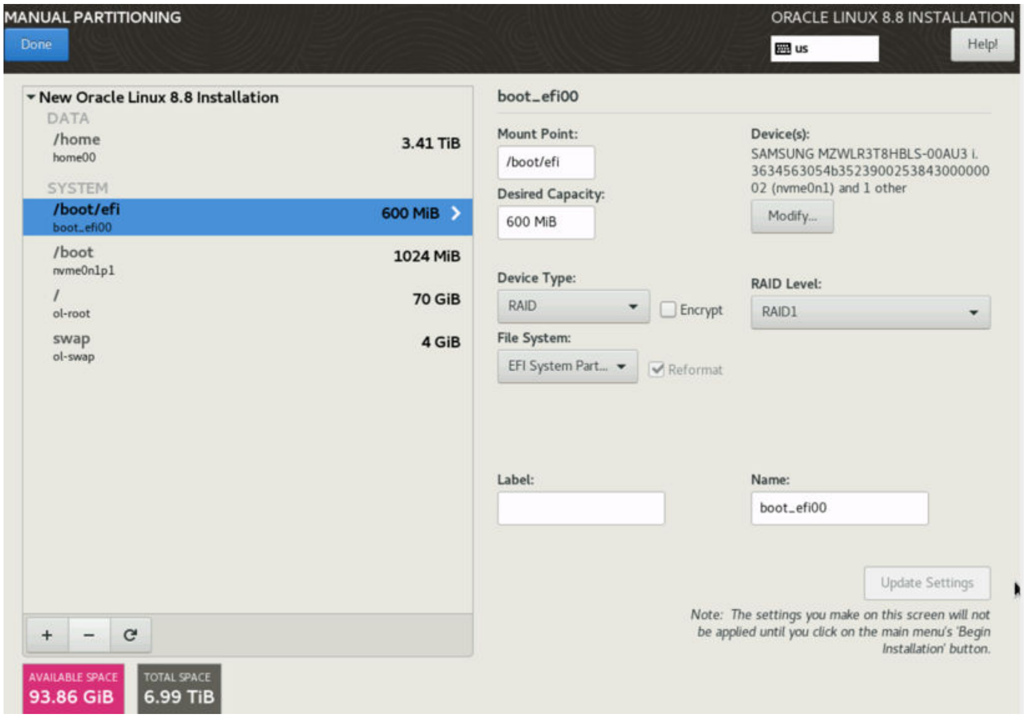
Label:

Name: home00

Update Settings

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

Figure 2-35 Manual partitioning boot efi



New Oracle Linux 8.8 Installation

DATA

/home home00	3.41 TiB

SYSTEM

/boot/efi boot_efi00	600 MiB
/boot nvme0n1p1	1024 MiB
/ ol-root	70 GiB
swap ol-swap	4 GiB

AVAILABLE SPACE 93.86 GiB

TOTAL SPACE 6.99 TiB

boot_efi00

Mount Point: /boot/efi

Desired Capacity: 600 MiB

Device(s): SAMSUNG MZWLR3T8HBLS-00AU3 i. 3634563054b35239002538430000002 (nvme0n1) and 1 other

Modify...

Device Type: RAID □ Encrypt

RAID Level: RAID1

File System: EFI System Part... ☑ Reformat

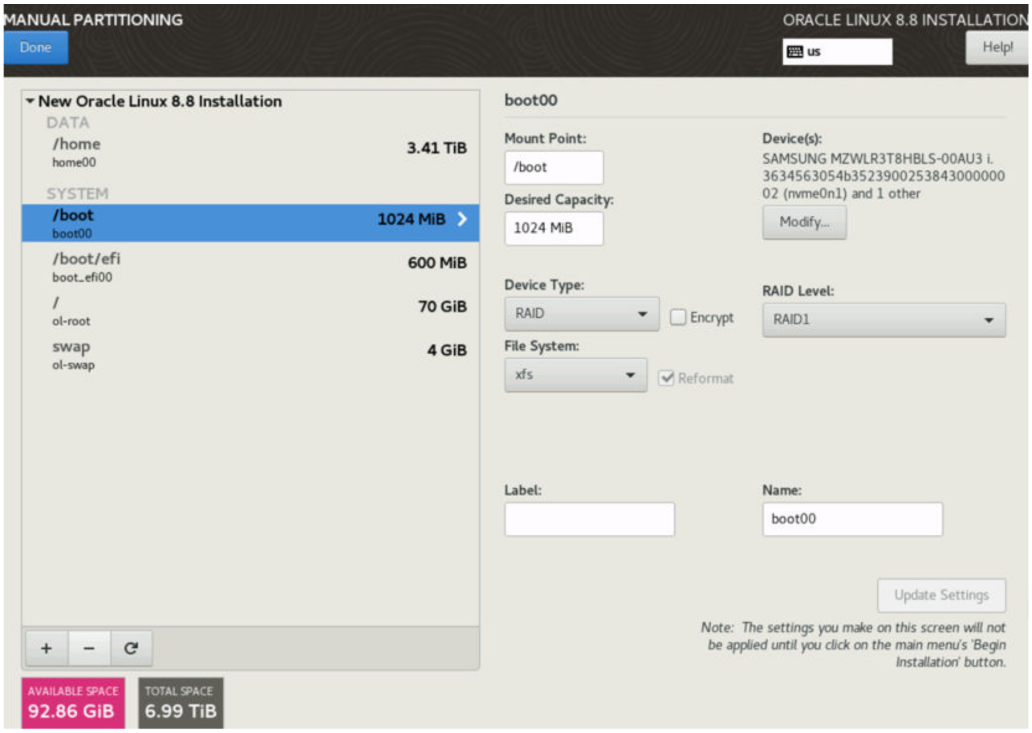
Label:

Name: boot_efi00

Update Settings

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

Figure 2-36 Manual partitioning boot



New Oracle Linux 8.8 Installation

DATA
/home home00 3.41 TiB

SYSTEM
/boot boot00 1024 MiB
/boot/efi boot_efi00 600 MiB
/ ol-root 70 GiB
swap ol-swap 4 GiB

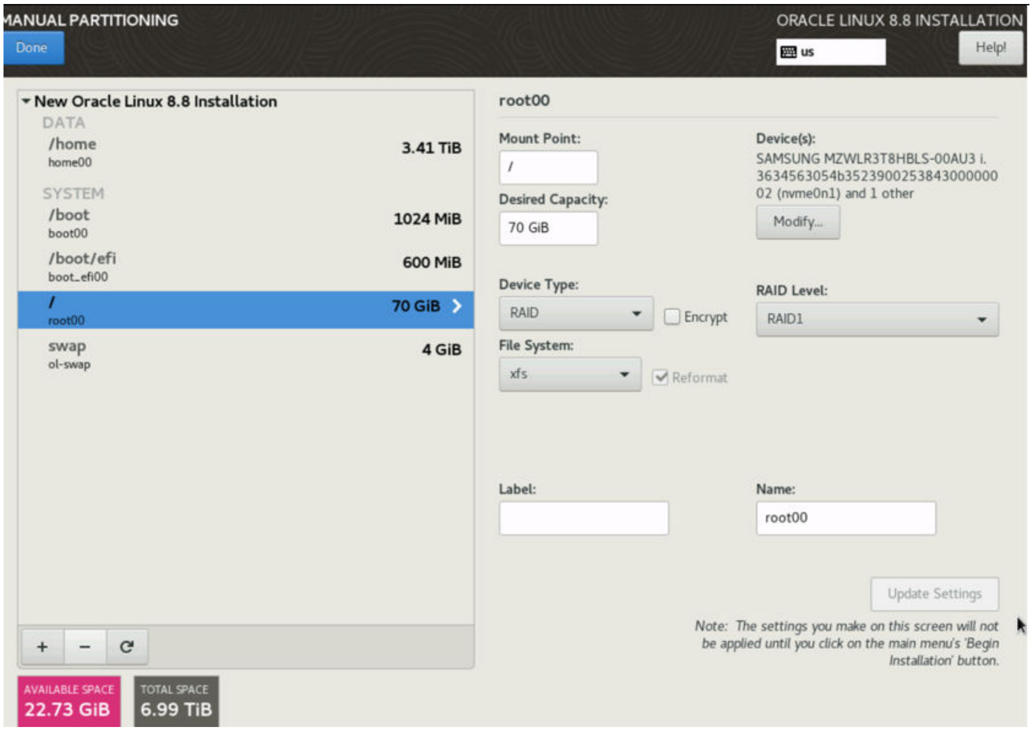
AVAILABLE SPACE 92.86 GiB
TOTAL SPACE 6.99 TiB

boot00

Mount Point: /boot
Desired Capacity: 1024 MiB
Device(s): SAMSUNG MZWLR3T8HBLS-00AU3 i. 3634563054b3523900253843000000 02 (nvme0n1) and 1 other
Device Type: RAID □ Encrypt
RAID Level: RAID1
File System: xfs ☑ Reformat
Label:
Name: boot00

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

Figure 2-37 Manual partitioning root



New Oracle Linux 8.8 Installation

DATA
/home home00 3.41 TiB

SYSTEM
/boot boot00 1024 MiB
/boot/efi boot_efi00 600 MiB
/ root00 70 GiB
swap ol-swap 4 GiB

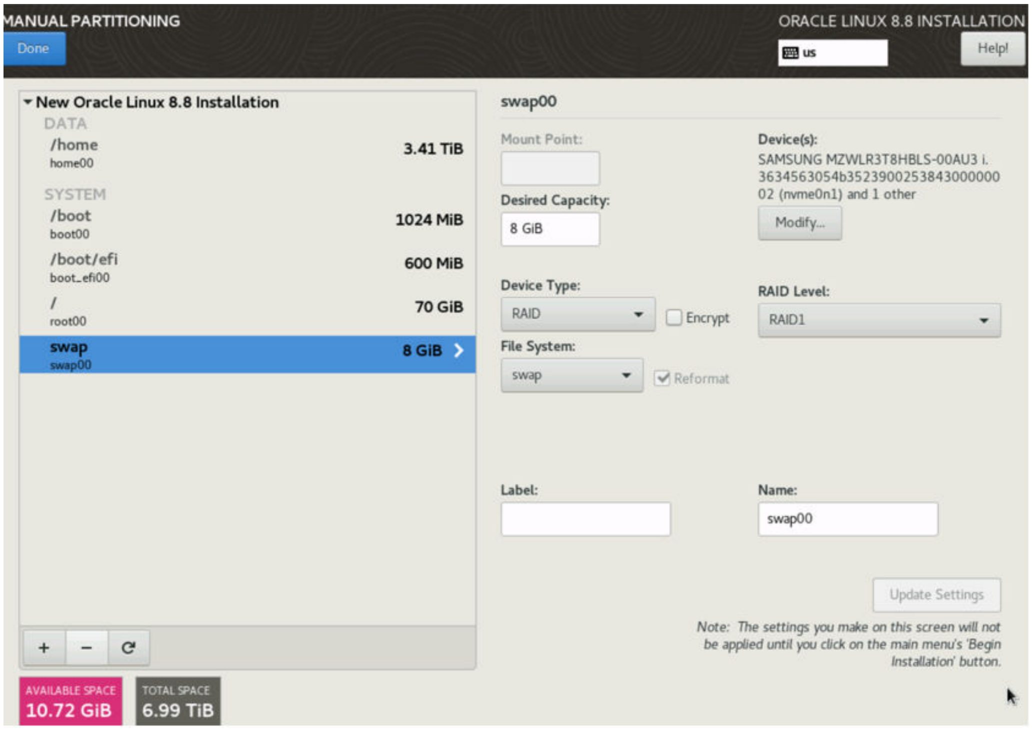
AVAILABLE SPACE 22.73 GiB
TOTAL SPACE 6.99 TiB

root00

Mount Point: /
Desired Capacity: 70 GiB
Device(s): SAMSUNG MZWLR3T8HBLS-00AU3 i. 3634563054b3523900253843000000 02 (nvme0n1) and 1 other
Device Type: RAID □ Encrypt
RAID Level: RAID1
File System: xfs ☑ Reformat
Label:
Name: root00

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

Figure 2-38 Manual partitioning swap



New Oracle Linux 8.8 Installation

DATA

/home home00	3.41 TiB

SYSTEM

/boot boot00	1024 MiB
/boot/efi boot_efi00	600 MiB
/ root00	70 GiB
swap swap00	8 GiB

swap00

Mount Point:

Desired Capacity: 8 GiB

Device(s): SAMSUNG MZWLR3T8HBLS-00AU3 i.3634563054b3523900253843000000 02 (nvme0n1) and 1 other

Device Type: RAID ☐ Encrypt

RAID Level: RAID1

File System: swap ☑ Reformat

Label:

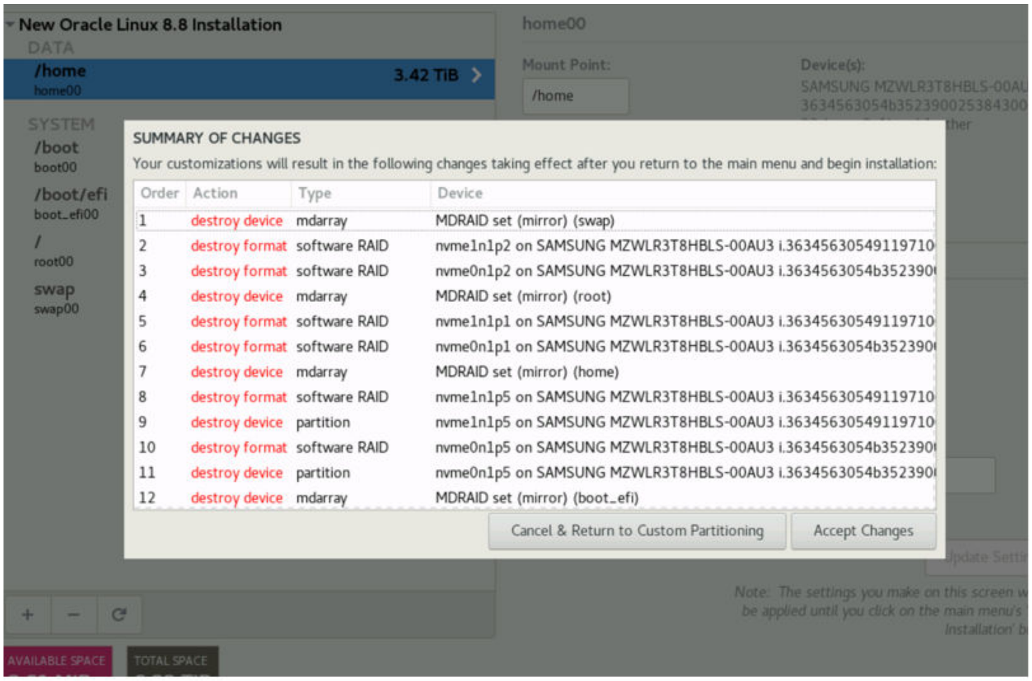
Name: swap00

Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.

AVAILABLE SPACE 10.72 GiB

TOTAL SPACE 6.99 TiB

Figure 2-39 Destroy device



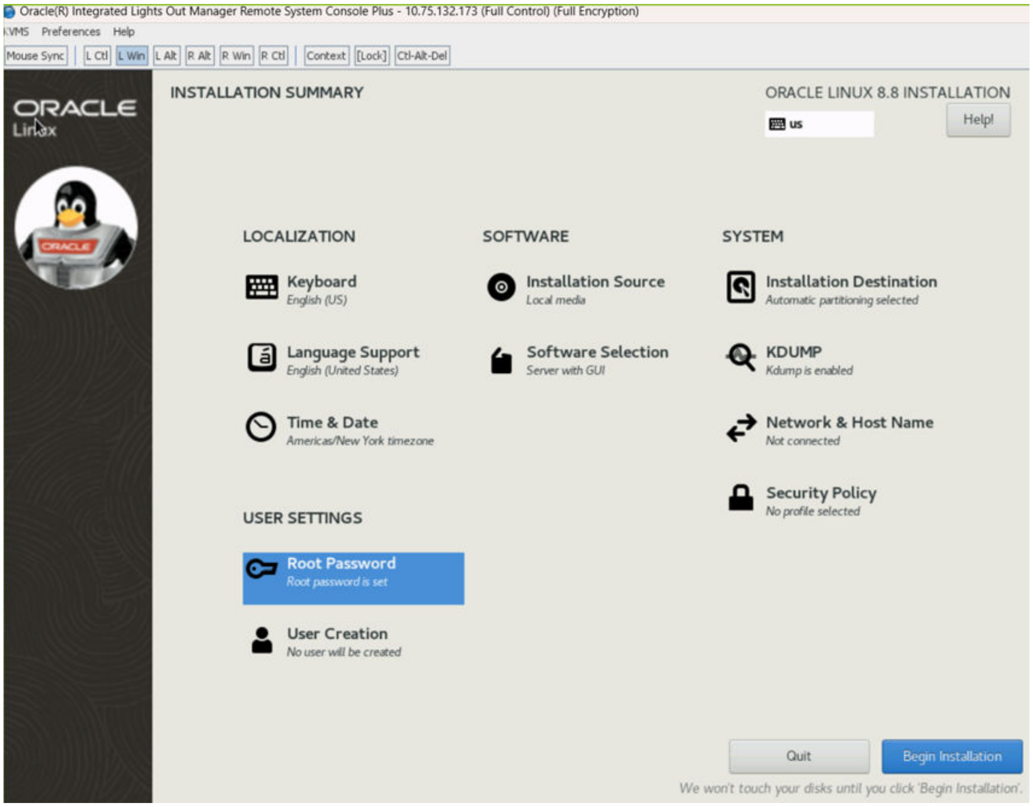
SUMMARY OF CHANGES

Your customizations will result in the following changes taking effect after you return to the main menu and begin installation:

Order	Action	Type	Device
1	destroy device	mdarray	MDRAID set (mirror) (swap)
2	destroy format	software RAID	nvme1n1p2 on SAMSUNG MZWLR3T8HBLS-00AU3 i.36345630549119710
3	destroy format	software RAID	nvme0n1p2 on SAMSUNG MZWLR3T8HBLS-00AU3 i.3634563054b352390
4	destroy device	mdarray	MDRAID set (mirror) (root)
5	destroy format	software RAID	nvme1n1p1 on SAMSUNG MZWLR3T8HBLS-00AU3 i.36345630549119710
6	destroy format	software RAID	nvme0n1p1 on SAMSUNG MZWLR3T8HBLS-00AU3 i.3634563054b352390
7	destroy device	mdarray	MDRAID set (mirror) (home)
8	destroy format	software RAID	nvme1n1p5 on SAMSUNG MZWLR3T8HBLS-00AU3 i.36345630549119710
9	destroy device	partition	nvme1n1p5 on SAMSUNG MZWLR3T8HBLS-00AU3 i.36345630549119710
10	destroy format	software RAID	nvme0n1p5 on SAMSUNG MZWLR3T8HBLS-00AU3 i.3634563054b352390
11	destroy device	partition	nvme0n1p5 on SAMSUNG MZWLR3T8HBLS-00AU3 i.3634563054b352390
12	destroy device	mdarray	MDRAID set (mirror) (boot_efi)

t. Select and enter information for **root password**.

Figure 2-40   Root password



Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryption)
KVMS Preferences Help
Mouse Sync | L Ctl | L Win | L Alt | R Alt | R Win | R Ctl | Context | [Lock] | Ctl-Alt-Del
ORACLE Linux
Help!
Quit
Begin Installation

INSTALLATION SUMMARY

ORACLE LINUX 8.8 INSTALLATION

us

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Installation Source
Local media

Software Selection
Server with GUI

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Not connected

Security Policy
No profile selected

USER SETTINGS

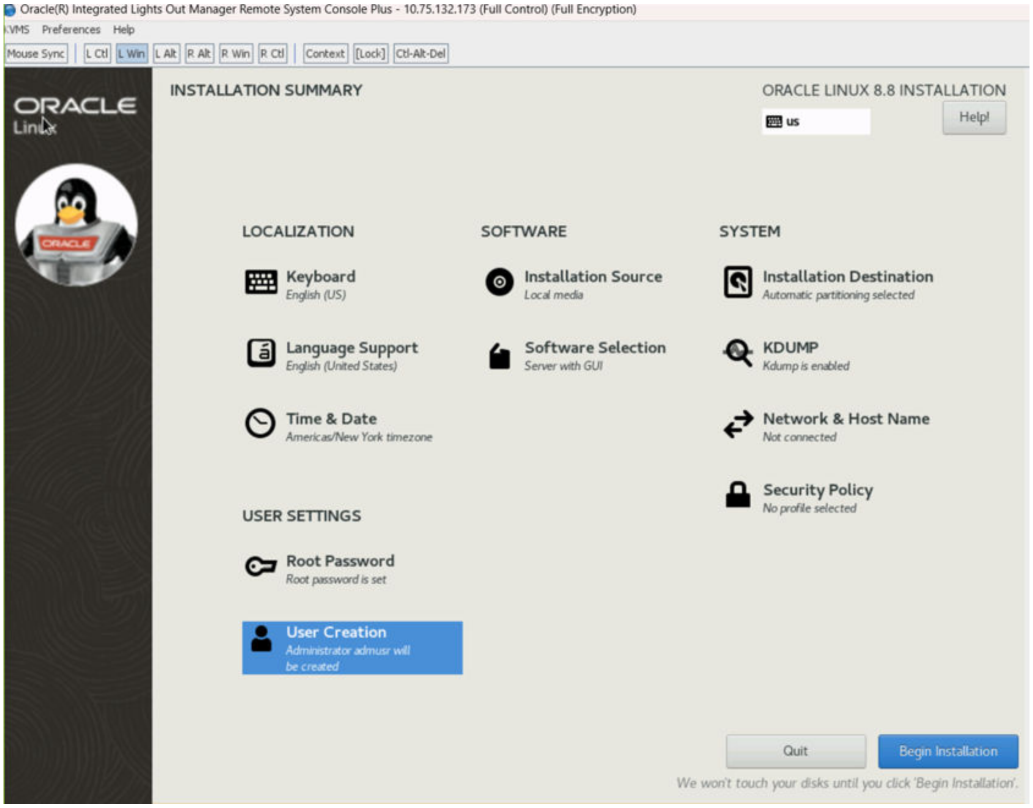
Root Password
Root password is set

User Creation
No user will be created

We won't touch your disks until you click 'Begin Installation'.

u. Select and enter information for **User Creation**.

Figure 2-41 User creation



INSTALLATION SUMMARY

ORACLE LINUX 8.8 INSTALLATION

us

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Installation Source
Local media

Software Selection
Server with GUI

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Not connected

Security Policy
No profile selected

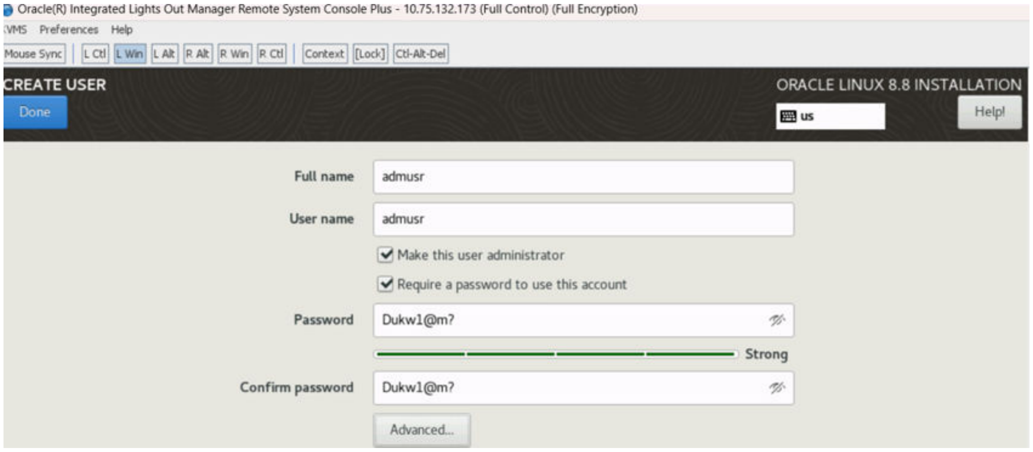
USER SETTINGS

Root Password
Root password is set

User Creation
Administrator admusr will be created

We won't touch your disks until you click 'Begin Installation'.

Figure 2-42 User example


Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryption)
KVMS Preferences Help
Mouse Sync
L Ctl
L Win
L Alt
R Alt
R Win
R Ctl
Context
[Lock]
Ctl-Alt-Del
Done
Help!
Advanced...

CREATE USER

ORACLE LINUX 8.8 INSTALLATION

us

Full name: admusr

User name: admusr

☑ Make this user administrator

☑ Require a password to use this account

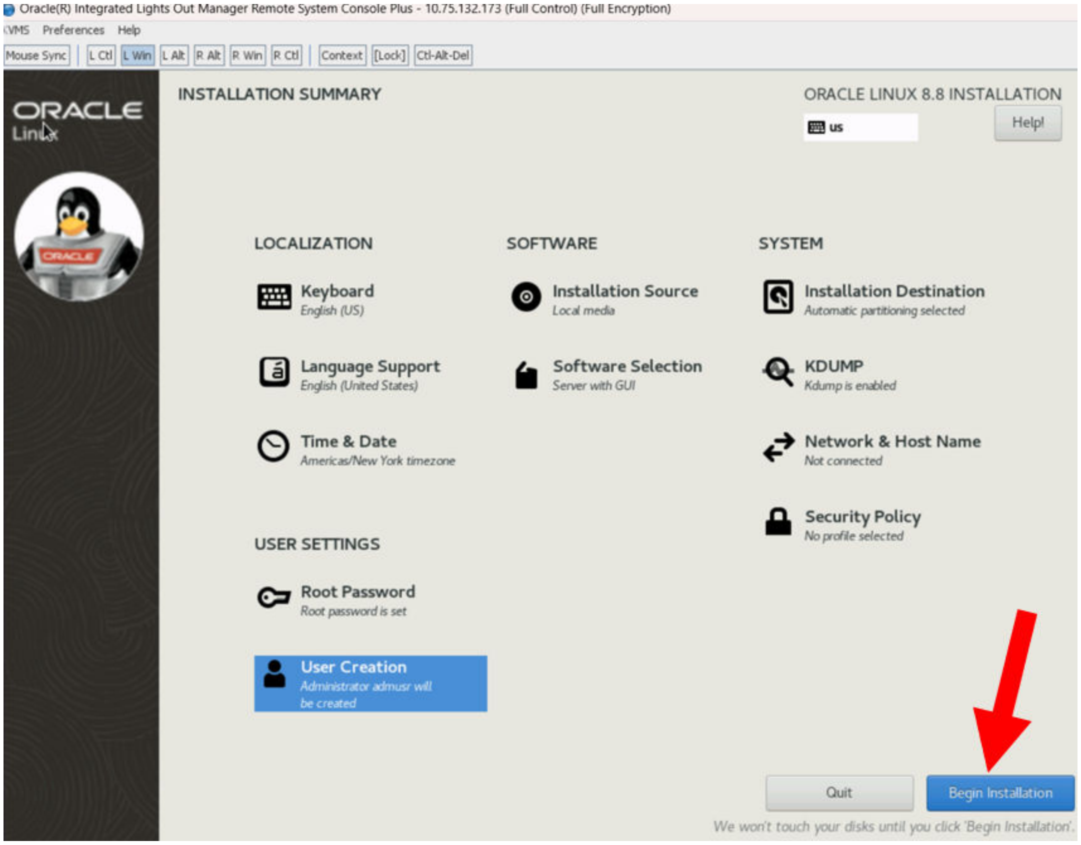
Password: Dukw1@m?

Strong

Confirm password: Dukw1@m?

9. Click **Begin Installation**

Figure 2-43   Begin installation



Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryption)

KVMS Preferences Help
Mouse Sync | L Ctl | L Win | L Alt | R Alt | R Win | R Ctl | Context | [Lock] | Ctl-Alt-Del
ORACLE Linux

INSTALLATION SUMMARY

ORACLE LINUX 8.8 INSTALLATION

LOCALIZATION

Keyboard
English (US)

Language Support
English (United States)

Time & Date
Americas/New York timezone

SOFTWARE

Installation Source
Local media

Software Selection
Server with GUI

SYSTEM

Installation Destination
Automatic partitioning selected

KDUMP
Kdump is enabled

Network & Host Name
Not connected

Security Policy
No profile selected

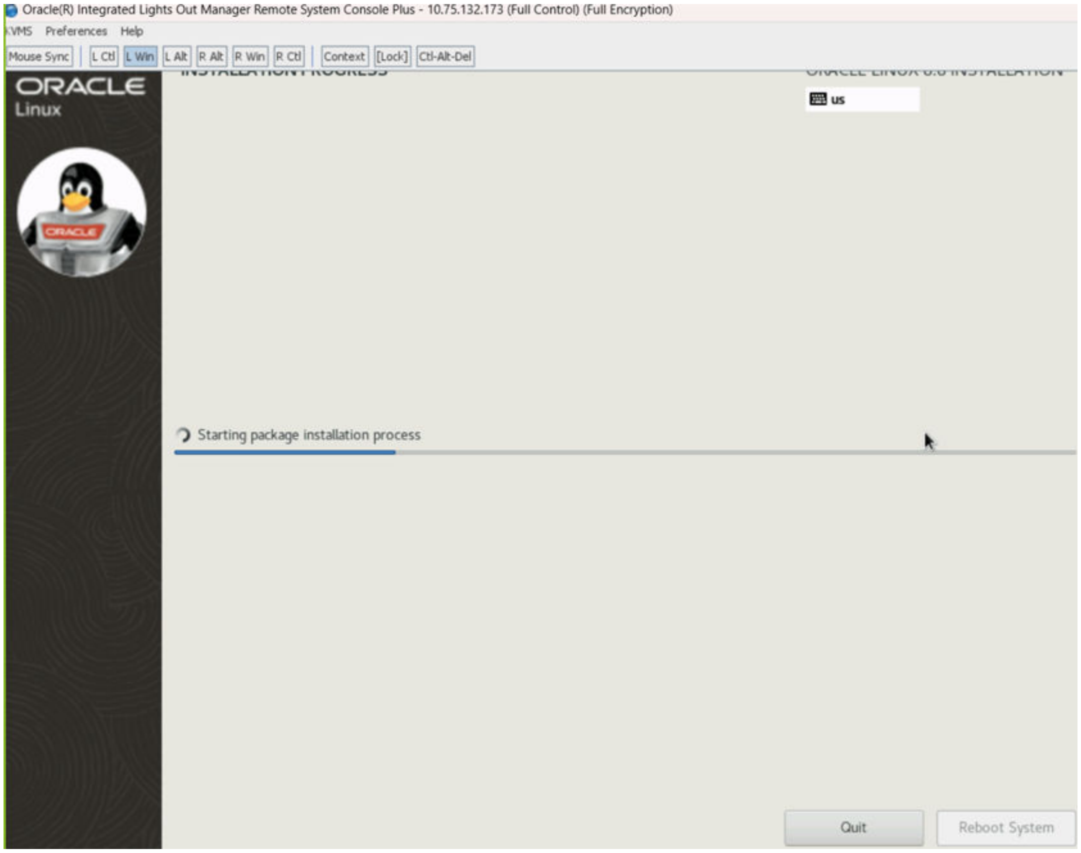
USER SETTINGS

Root Password
Root password is set

User Creation
Administrator admusr will be created

We won't touch your disks until you click 'Begin Installation'.

Figure 2-44   Starting package installation progress



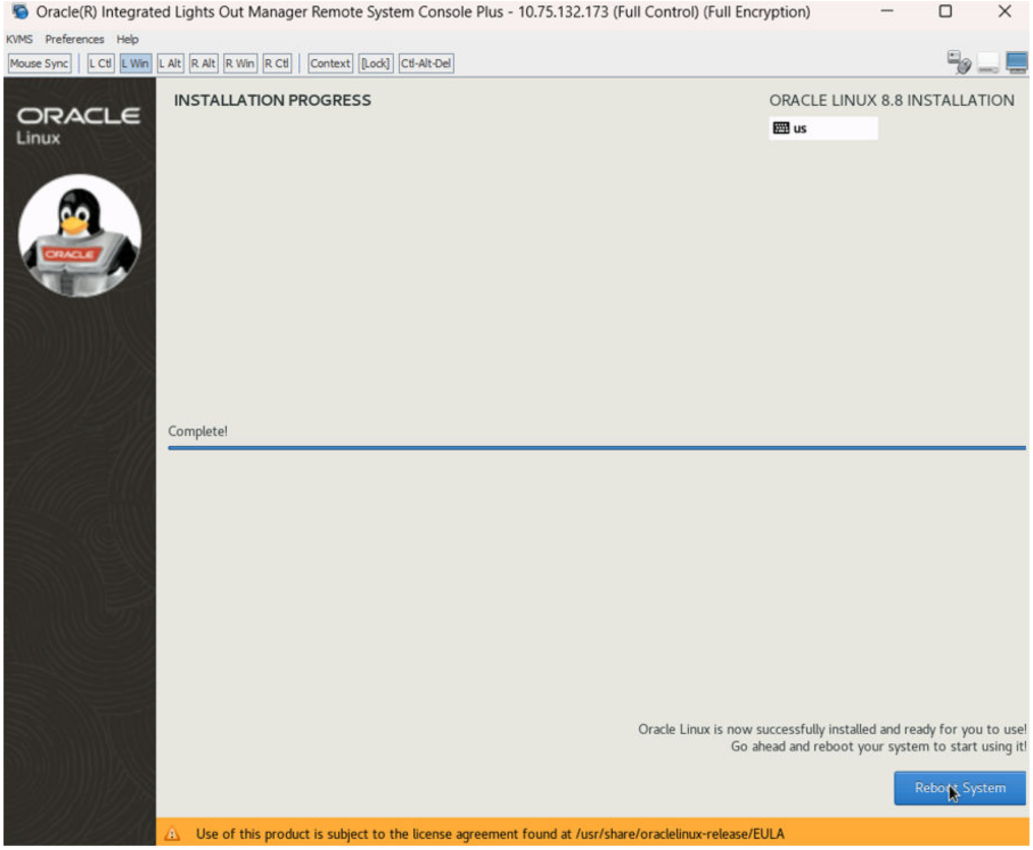
Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryption)
KVMS Preferences Help
Mouse Sync | L Ctl | L Win | L Alt | R Alt | R Win | R Ctl | Context | [Lock] | Ctl-Alt-Del
ORACLE Linux
INSTALLATION PROGRESS
ORACLE LINUX 8.8 INSTALLATION
us
Quit
Reboot System

Starting package installation process

10. Reboot after installation

    - When OL8.x installation is complete, you are prompted to reboot server and start OL8.x.

Figure 2-45   Installation progress



Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryption)
KVMS
Preferences
Help
Mouse Sync
L Ctl
L Win
L Alt
R Alt
R Win
R Ctl
Context
[Lock]
Ctl-Alt-Del
ORACLE
Linux
INSTALLATION PROGRESS
ORACLE LINUX 8.8 INSTALLATION
us
Reboot System

Complete!

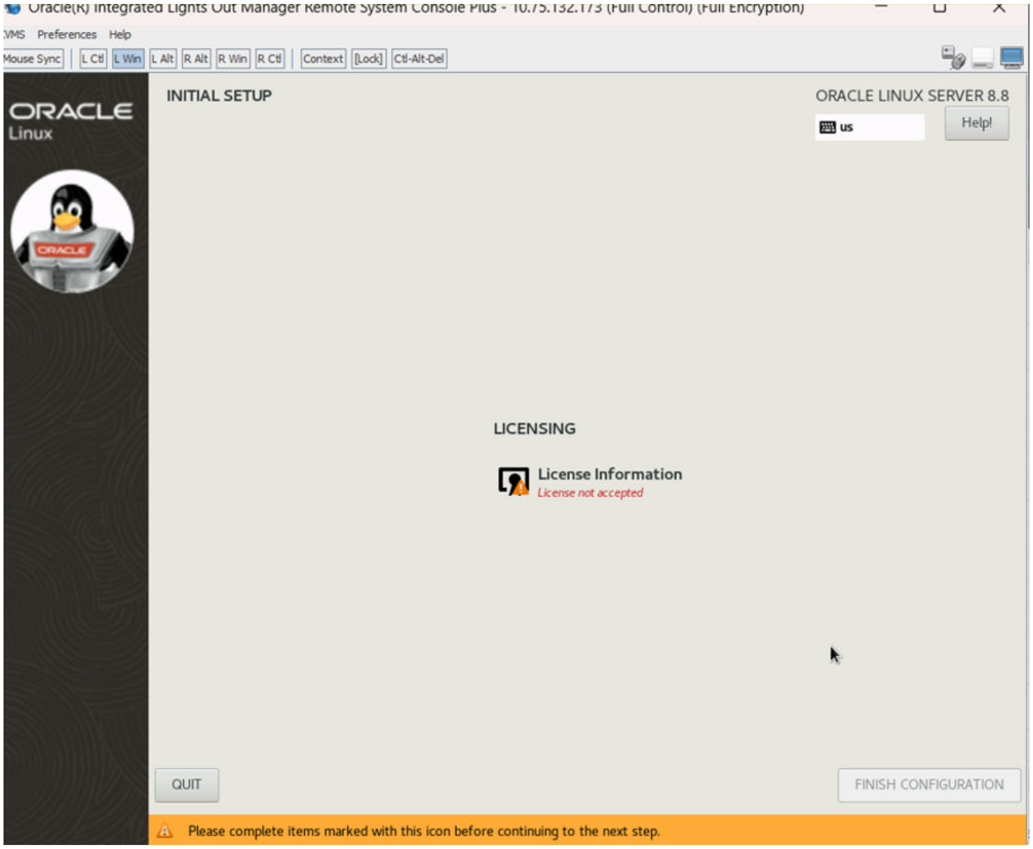
Oracle Linux is now successfully installed and ready for you to use!
Go ahead and reboot your system to start using it!

Use of this product is subject to the license agreement found at /usr/share/oraclelinux-release/EULA

11. Select License

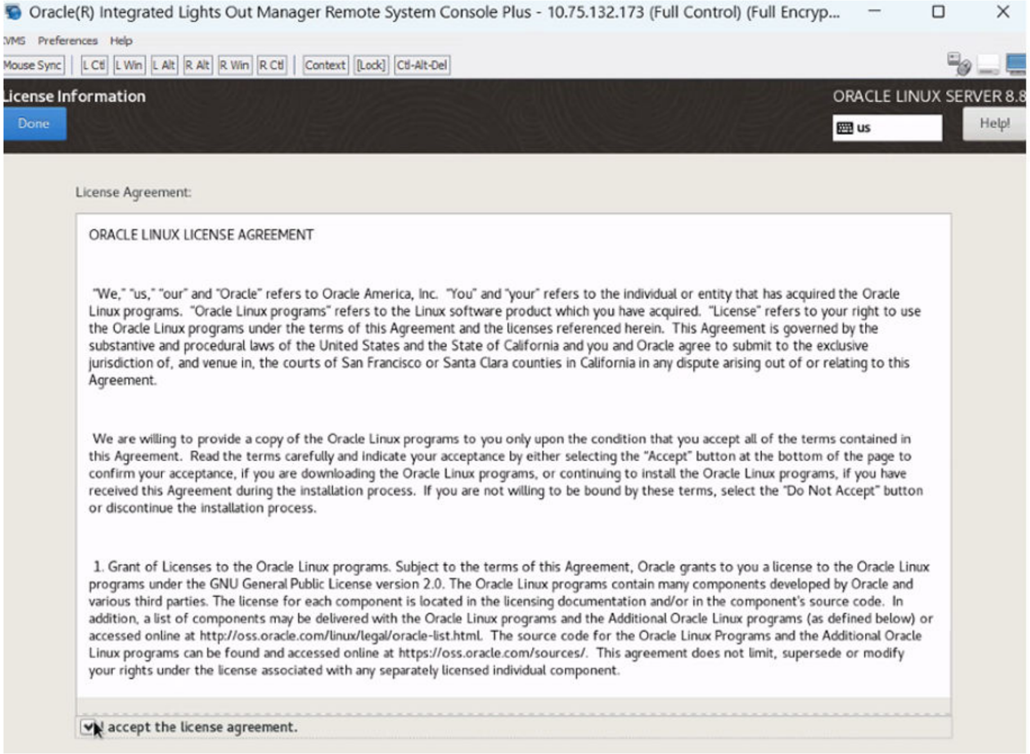
    a. Check in the box I accept the license agreement to accept the license.

Figure 2-46 License



b. License will change to Accepted.

Figure 2-47   Licence acceptance


Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryp...
KVMS Preferences Help
Mouse Sync L Ctl L Win L Alt R Alt R Win R Ctl Context [Lock] Ctl-Alt-Del
License Information
Done
ORACLE LINUX SERVER 8.8
us
Help!

License Agreement:

ORACLE LINUX LICENSE AGREEMENT

"We," "us," "our" and "Oracle" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that has acquired the Oracle Linux programs. "Oracle Linux programs" refers to the Linux software product which you have acquired. "License" refers to your right to use the Oracle Linux programs under the terms of this Agreement and the licenses referenced herein. This Agreement is governed by the substantive and procedural laws of the United States and the State of California and you and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

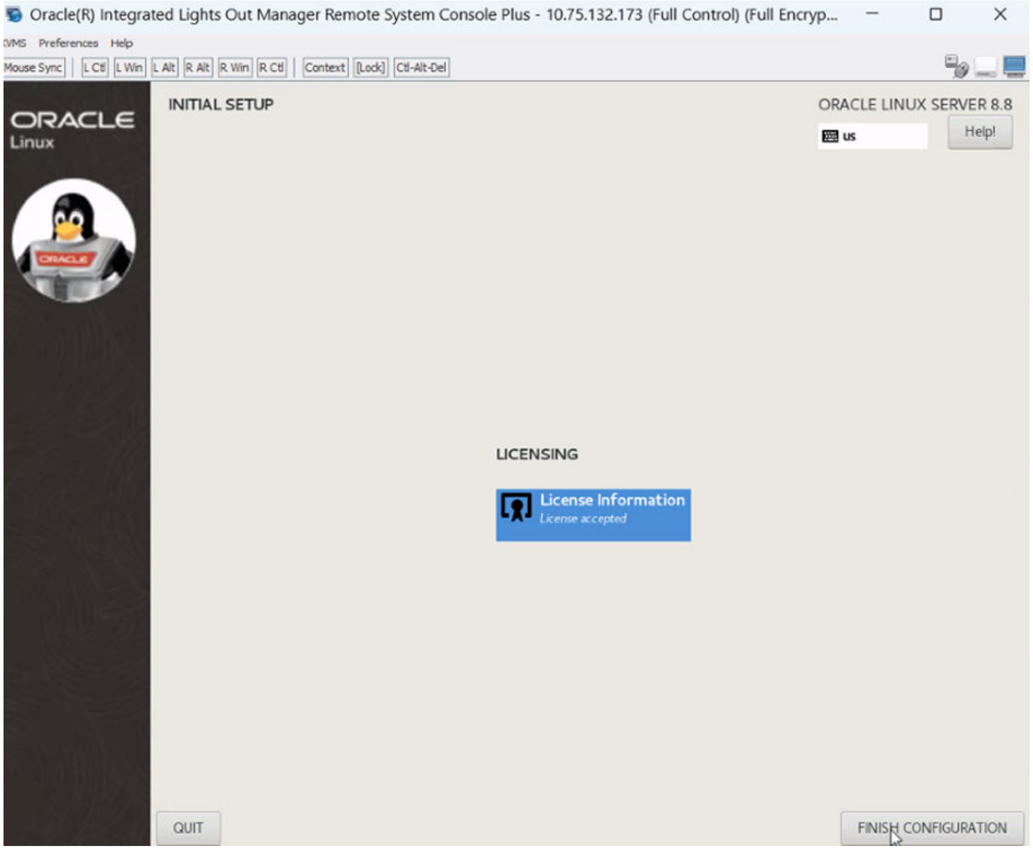
We are willing to provide a copy of the Oracle Linux programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and indicate your acceptance by either selecting the "Accept" button at the bottom of the page to confirm your acceptance, if you are downloading the Oracle Linux programs, or continuing to install the Oracle Linux programs, if you have received this Agreement during the installation process. If you are not willing to be bound by these terms, select the "Do Not Accept" button or discontinue the installation process.

1. Grant of Licenses to the Oracle Linux programs. Subject to the terms of this Agreement, Oracle grants to you a license to the Oracle Linux programs under the GNU General Public License version 2.0. The Oracle Linux programs contain many components developed by Oracle and various third parties. The license for each component is located in the licensing documentation and/or in the component's source code. In addition, a list of components may be delivered with the Oracle Linux programs and the Additional Oracle Linux programs (as defined below) or accessed online at http://oss.oracle.com/linux/legal/oracle-list.html. The source code for the Oracle Linux Programs and the Additional Oracle Linux programs can be found and accessed online at https://oss.oracle.com/sources/. This agreement does not limit, supersede or modify your rights under the license associated with any separately licensed individual component.

☑ I accept the license agreement.

c. Select **FINISH CONFIGURATION** to complete.

Figure 2-48   License Configuration


Oracle(R) Integrated Lights Out Manager Remote System Console Plus - 10.75.132.173 (Full Control) (Full Encryp...
KVMS Preferences Help
Mouse Sync | L Ctl | L Win | L Alt | R Alt | R Win | R Ctl | Context | Lock | Ctl-Alt-Del
ORACLE Linux
INITIAL SETUP
ORACLE LINUX SERVER 8.8
us
Help!
LICENSING
License Information
License accepted
QUIT
FINISH CONFIGURATION

12. Verify kernel version and KVM version:

- Open terminal console window and verify the following commands in the code:

  i. `$ uname -a`

  ii. `$ virsh version`

```
cat /etc/os-release
NAME="Oracle Linux Server"
VERSION="8.8"
ID="ol"
ID_LIKE="fedora"
VARIANT="Server"
VARIANT_ID="server"
VERSION_ID="8.8"
PLATFORM_ID="platform:el8"
PRETTY_NAME="Oracle Linux Server 8.8"
ANSI_COLOR="0;31"
CPE_NAME="cpe:/o:oracle:linux:8:8:server"
HOME_URL="https://linux.oracle.com/"
BUG_REPORT_URL="https://bugzilla.oracle.com/"
ORACLE_BUGZILLA_PRODUCT="Oracle Linux 8"
ORACLE_BUGZILLA_PRODUCT_VERSION=8.8
ORACLE_SUPPORT_PRODUCT="Oracle Linux"
```

```
ORACLE_SUPPORT_PRODUCT_VERSION=8.8
[2:49 PM] Linux sentinel6-6 5.15.0-101.103.2.1.el8uek.x86_64 #2 SMP Mon
May 1 20:11:30 PDT 2023 x86_64 x86_64 x86_64 GNU/Linux
Using library: libvirt 8.0.0
Using API: QEMU 8.0.0
Running hypervisor: QEMU 6.2.0
Linux sentinel6-6 5.15.0-101.103.2.1.el8uek.x86_64
```

13. Disconnect the ISO from storage if Step 3 is followed, if not skip the following step From ILOM Console, Go to `KVMS/Storage`, select the ISO and then select disconnect.

2.5 DSR Installation of OL8 and KVM on Gen 10

DSR Installation on OL8 and KVM includes the following procedures:

- Installing DSR on Linux/KVM
- Creating and installing OCDSR VMs through KVM GUI

> **Note**
>
> If using a hardware in remote Lab, then use a remote windows machine to install Linux, ensure that OEL 8 ISO is also located locally in remote windows machine.

2.5.1 Installing DSR on OL8 and KVM

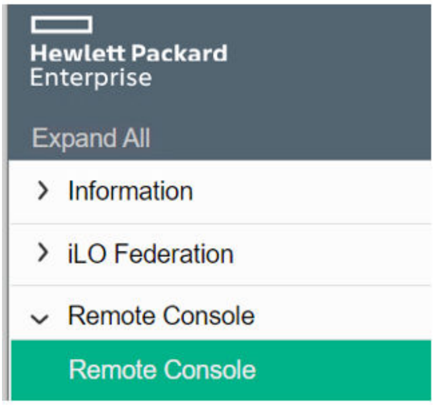
This procedure lists the steps to install DSR configuration on Oracle Linux OS with direct KVM as hypervisor.

> **Note**
>
> - This installation procedure only applies while installing DSR on Oracle Linux OS through direct KVM.
> - For the Oracle Linux OS, Oracle Linux 8.x release is used and verified.
> - The screenshots shared in this procedure are taken from HP Gen-10 Blade.
> - This procedure can run on any flavor of blade that requires DSR install on OL8.x and KVM.
> - Perform this procedure on each blade.

Prerequisites:
All the respective infrastructures have to be up and running.

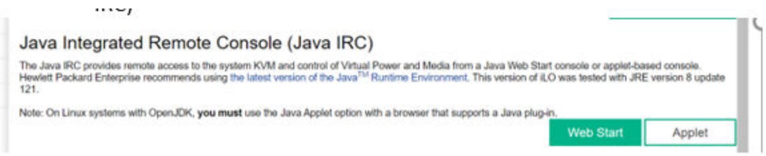
1. To mount virtual media containing Oracle Linux OS software, perform the following steps:
   a. Open **iLO** GUI.
   b. Click **Remote Consoles** on the left pane menu.

Figure 2-49 Remote Console



c. Click **Web Start** under Java Integrated Remote Console (Java IRC).

Figure 2-50 Java IRC



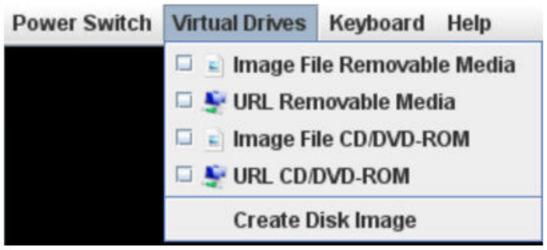
Java Integrated Remote Console (Java IRC)

The Java IRC provides remote access to the system KVM and control of Virtual Power and Media from a Java Web Start console or applet-based console. Hewlett Packard Enterprise recommends using the latest version of the Java^{TM} Runtime Environment. This version of iLO was tested with JRE version 8 update 121.

Note: On Linux systems with OpenJDK, **you must** use the Java Applet option with a browser that supports a Java plug-in.

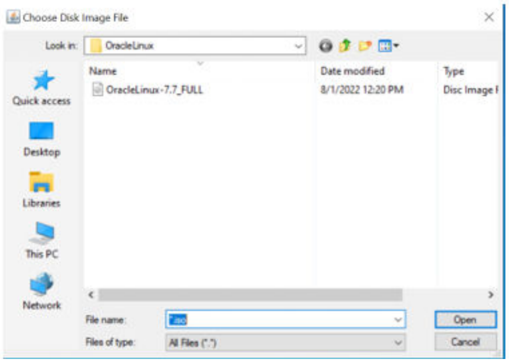
d. Navigate to **Virtual Drives** and select **Image File CD-ROM/DVD**.

Figure 2-51 Virtual Drives



e. Browse and select the Oracle Linux 8 image file.

Figure 2-52 Browse Oracle Linux 8.x file



Choose Disk Image File

Look in: OracleLinux

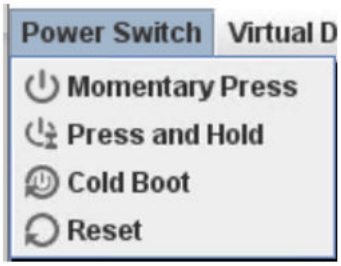
Name	Date modified	Type
OracleLinux-7.7_FULL	8/1/2022 12:20 PM	Disc Image F

File name: *.iso

Files of type: All Files (*.*)

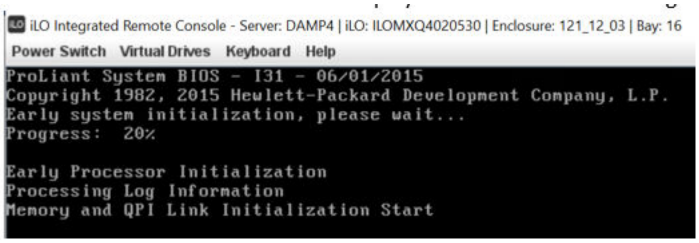
2. To reboot host, perform the following steps:
   a. Log in to **Blade Server iLO** GUI browser page and launch remote console.
   b. Click **Power Switch** and select **Reset** from the drop-down menu.

Figure 2-53 Power Switch



   c. Click **Ok** to confirm reset.
   d. The **Remote Console** window displays that the host is rebooting.

Figure 2-54 Host rebooting


iLO Integrated Remote Console - Server: DAMP4 | iLO: ILOMXQ4020530 | Enclosure: 121_12_03 | Bay: 16
Power Switch
Virtual Drives
Keyboard
Help

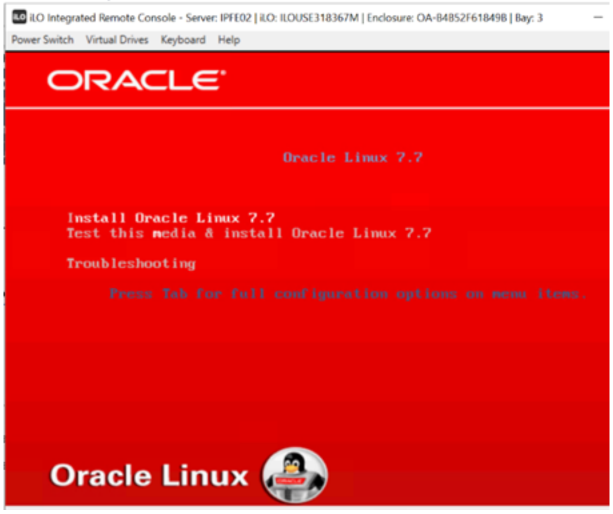
```
ProLiant System BIOS - I31 - 06/01/2015
Copyright 1982, 2015 Hewlett-Packard Development Company, L.P.
Early system initialization, please wait...
Progress:  20%

Early Processor Initialization
Processing Log Information
Memory and QPI Link Initialization Start
```

Wait for a couple of minutes for reboot to complete.

Once reboot completes, the host boots with Oracle Linux installation ISO and the GUI screen prompts for the installation options.

3. To initiate Oracle Linux Platform installation, select **Install Oracle Linux 8.x** to continue.

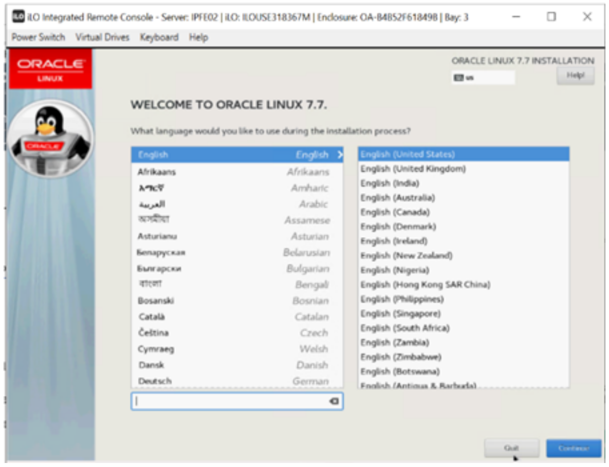
Figure 2-55 Installation Options


iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F61849B | Bay: 3
Power Switch
Virtual Drives
Keyboard
Help
ORACLE
Oracle Linux

```
                    Oracle Linux 7.7

Install Oracle Linux 7.7
Test this media & install Oracle Linux 7.7

Troubleshooting

     Press Tab for full configuration options on menu items.
```

4. To choose Oracle Linux OS language, select **English** as Oracle Linux OS language and click **Continue** to go to next step.

Figure 2-56 Language Selection


iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F618498 | Bay: 3
Power Switch
Virtual Drives
Keyboard
Help
ORACLE LINUX
ORACLE LINUX 7.7 INSTALLATION
us
Help!
Quit
Continue

WELCOME TO ORACLE LINUX 7.7.

What language would you like to use during the installation process?

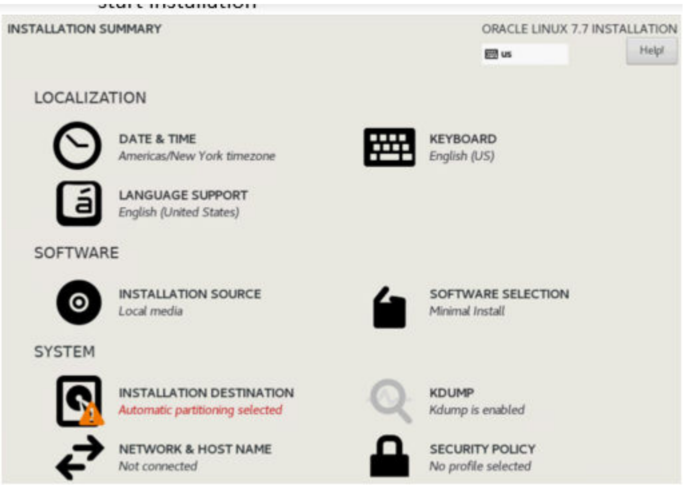
English	English
Afrikaans	Afrikaans
አማርኛ	Amharic
العربية	Arabic
অসমীয়া	Assamese
Asturianu	Asturian
Беларуская	Belarusian
Български	Bulgarian
বাংলা	Bengali
Bosanski	Bosnian
Català	Catalan
Čeština	Czech
Cymraeg	Welsh
Dansk	Danish
Deutsch	German

English (United States)
English (United Kingdom)
English (India)
English (Australia)
English (Canada)
English (Denmark)
English (Ireland)
English (New Zealand)
English (Nigeria)
English (Hong Kong SAR China)
English (Philippines)
English (Singapore)
English (South Africa)
English (Zambia)
English (Zimbabwe)
English (Botswana)
English (Antigua & Barbuda)

The next page **INSTALLATION SUMMARY** displays the required information to start installation.

5. To set up time zone, click **DATE & TIME** under **LOCALIZATION**.

Figure 2-57 Installation Summary



INSTALLATION SUMMARY

LOCALIZATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Minimal Install

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

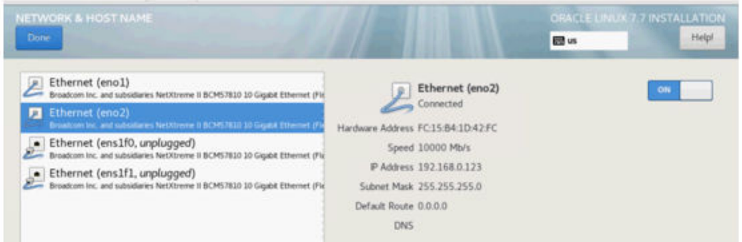
KDUMP
Kdump is enabled

NETWORK & HOST NAME
Not connected

SECURITY POLICY
No profile selected

a. Click **Network & Hostname** under System and ensure that the system is connected to a network.

Figure 2-58   Network and hostname



Ethernet (eno1)
Broadcom Inc. and subsidiaries NetXtreme II BCM57810 10 Gigabit Ethernet (Fi

Ethernet (eno2)
Broadcom Inc. and subsidiaries NetXtreme II BCM57810 10 Gigabit Ethernet (Fi

Ethernet (ens1f0, unplugged)
Broadcom Inc. and subsidiaries NetXtreme II BCM57810 10 Gigabit Ethernet (Fi

Ethernet (ens1f1, unplugged)
Broadcom Inc. and subsidiaries NetXtreme II BCM57810 10 Gigabit Ethernet (Fi

Ethernet (eno2)
Connected

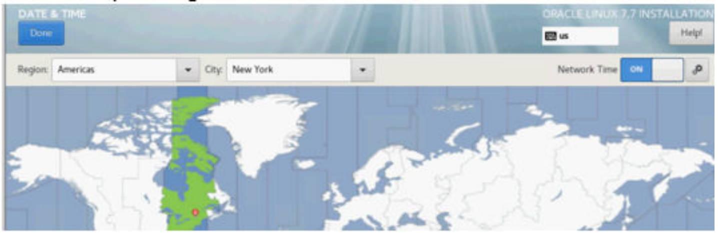
Hardware Address FC:15:B4:1D:42:FC
Speed 10000 Mb/s
IP Address 192.168.0.123
Subnet Mask 255.255.255.0
Default Route 0.0.0.0
DNS

b. Click **Done** to continue.

c. Click **Localizationà Date & Time**.

d. Pick a time zone by selecting a region and city from the drop-down list, or by clicking location on the map.

Figure 2-59   Date and Time

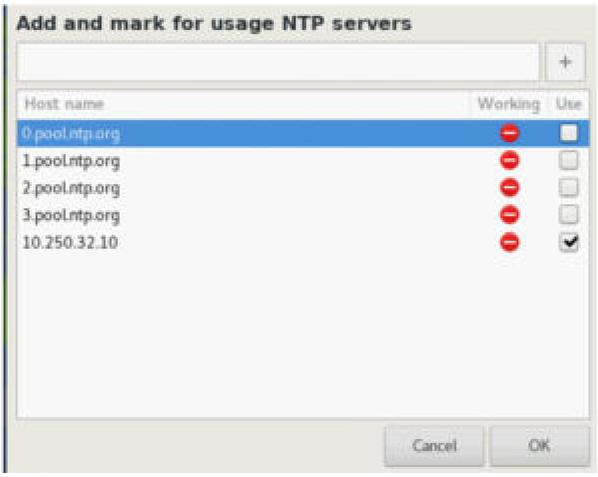


Region: Americas
City: New York
Network Time ON

e. Toggle the switch to turn **ON** Network Time.

f. Click **Settings**, configure the NTP servers used by the system.

Figure 2-60   Add and mark for usage NTP servers



Add and mark for usage NTP servers

Host name	Working	Use
0.pool.ntp.org	⛔	☐
1.pool.ntp.org	⛔	☐
2.pool.ntp.org	⛔	☐
3.pool.ntp.org	⛔	☐
10.250.32.10	⛔	☑

g. Click **Ok** to go back to the previous screen.

h. Click **Done** to continue.

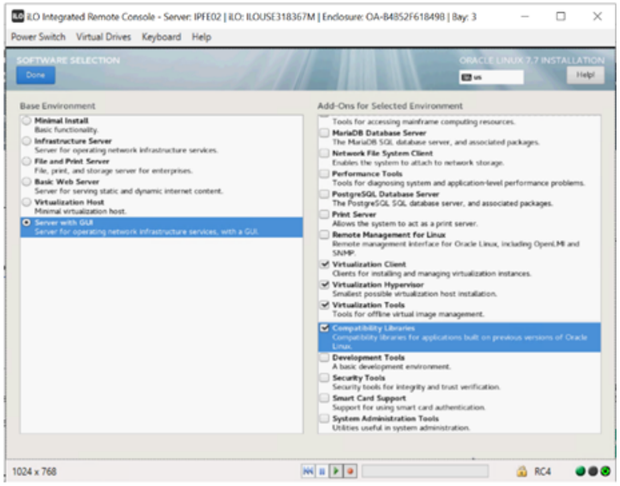
6. To set up installation on base environment, perform the following steps:

   a. Click **SOFTWARE SELECTION** option in the **SOFTWARE** area.

b. Select **Server with GUI** from the **Base Environment** area, and ensure that the following add-ons are selected:

- Virtualization Client
- Virtualization Hypervisor
- Virtualization Tools
- Compatibility Libraries

Figure 2-61 Software Selection


iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4852F618498 | Bay: 3
Power Switch
Virtual Drives
Keyboard
Help
SOFTWARE SELECTION
Done
ORACLE LINUX 7.7 INSTALLATION
us
Help!
1024 x 768
RC4

Base Environment

○ **Minimal Install**
Basic functionality.
○ **Infrastructure Server**
Server for operating network infrastructure services.
○ **File and Print Server**
File, print, and storage server for enterprises.
○ **Basic Web Server**
Server for serving static and dynamic internet content.
○ **Virtualization Host**
Minimal virtualization host.
● **Server with GUI**
Server for operating network infrastructure services, with a GUI.

Add-Ons for Selected Environment

Tools for accessing mainframe computing resources.
□ **MariaDB Database Server**
The MariaDB SQL database server, and associated packages.
□ **Network File System Client**
Enables the system to attach to network storage.
□ **Performance Tools**
Tools for diagnosing system and application-level performance problems.
□ **PostgreSQL Database Server**
The PostgreSQL SQL database server, and associated packages.
□ **Print Server**
Allows the system to act as a print server.
□ **Remote Management for Linux**
Remote management interface for Oracle Linux, including OpenLMI and SNMP.
☑ **Virtualization Client**
Clients for installing and managing virtualization instances.
☑ **Virtualization Hypervisor**
Smallest possible virtualization host installation.
☑ **Virtualization Tools**
Tools for offline virtual image management.
☑ **Compatibility Libraries**
Compatibility libraries for applications built on previous versions of Oracle Linux.
□ **Development Tools**
A basic development environment.
□ **Security Tools**
Security tools for integrity and trust verification.
□ **Smart Card Support**
Support for using smart card authentication.
□ **System Administration Tools**
Utilities useful in system administration.

c. Click **Done** to save the changes and go back to the main configuration page.

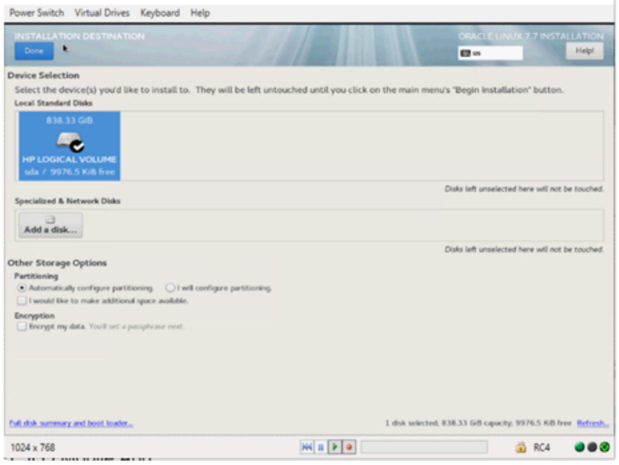
7. To setup installation destination, click **INSTALLATION DESTINATION** in the **SYSTEM** area, then perform the following steps:

   a. Select **sda** or **sdb** to be used.

   b. Check **Automatically configure partitioning**.

   c. Click **Done** to continue.

Figure 2-62 Installation Destination



Device Selection

Select the device(s) you'd like to install to. They will be left untouched until you click on the main menu's "Begin Installation" button.

Local Standard Disks

838.33 GiB
HP LOGICAL VOLUME
sda / 9976.5 KiB free

Disks left unselected here will not be touched.

Specialized & Network Disks

Disks left unselected here will not be touched.

Other Storage Options

Partitioning

● Automatically configure partitioning. ○ I will configure partitioning.
□ I would like to make additional space available.

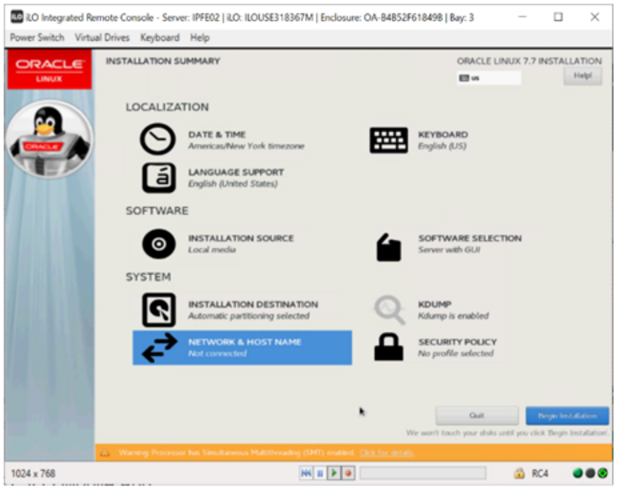
Encryption

□ Encrypt my data. *You'll set a passphrase next.*

1 disk selected; 838.33 GiB capacity; 9976.5 KiB free

8. To start installation, review all the information and click **Begin Installation**.

Figure 2-63 Installation Summary


iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F61849B | Bay: 3
Power Switch
Virtual Drives
Keyboard
Help
ORACLE LINUX
ORACLE LINUX 7.7 INSTALLATION
us
Help!
Quit
Begin Installation
1024 x 768
RC4

INSTALLATION SUMMARY

LOCALIZATION

DATE & TIME
Americas/New York timezone

KEYBOARD
English (US)

LANGUAGE SUPPORT
English (United States)

SOFTWARE

INSTALLATION SOURCE
Local media

SOFTWARE SELECTION
Server with GUI

SYSTEM

INSTALLATION DESTINATION
Automatic partitioning selected

KDUMP
Kdump is enabled

NETWORK & HOST NAME
Not connected

SECURITY POLICY
No profile selected

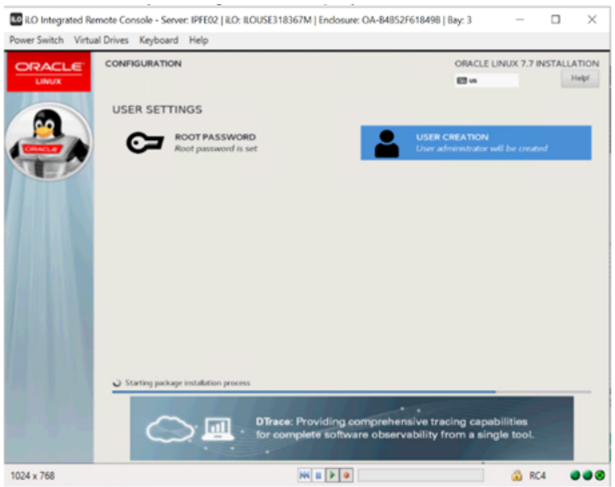
We won't touch your disks until you click Begin Installation.

Warning: Processor has Simultaneous Multithreading (SMT) enabled. Click for details.

> **Note**
>
> Network configuration is not mandatory at this point and can be performed after Oracle Linux OS is installed.

9. To create login credentials, configure root credential or any other login credentials as required.

Figure 2-64 Login Credential Configuration


iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F61849B | Bay: 3
Power Switch
Virtual Drives
Keyboard
Help
ORACLE LINUX
ORACLE LINUX 7.7 INSTALLATION
us
Help!
DTrace: Providing comprehensive tracing capabilities for complete software observability from a single tool.
1024 x 768
RC4

CONFIGURATION

USER SETTINGS

ROOT PASSWORD
Root password is set

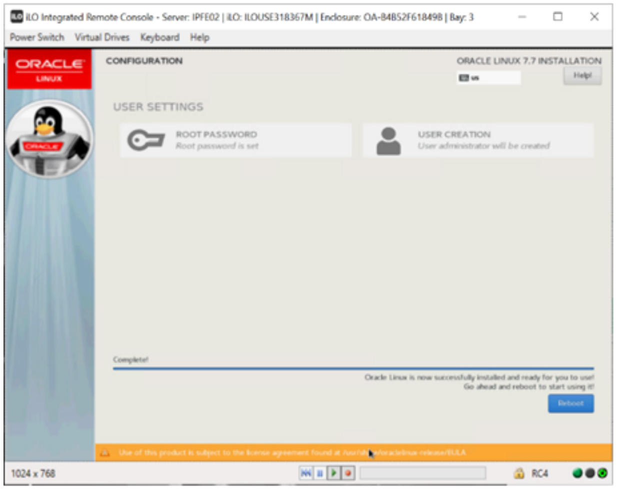
USER CREATION
User administrator will be created

Starting package installation process

> **Note**
>
> At the same time Oracle Linux installation software lays down files into Gen 10 local hard disk.

Wait for the installation to complete until the following screen appears.

Figure 2-65 Installation Configured


iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F618498 | Bay: 3
Power Switch
Virtual Drives
Keyboard
Help
ORACLE LINUX
CONFIGURATION
ORACLE LINUX 7.7 INSTALLATION
us
Help!
USER SETTINGS
ROOT PASSWORD
USER CREATION
Reboot
1024 x 768
RC4

Root password is set

User administrator will be created

Complete!

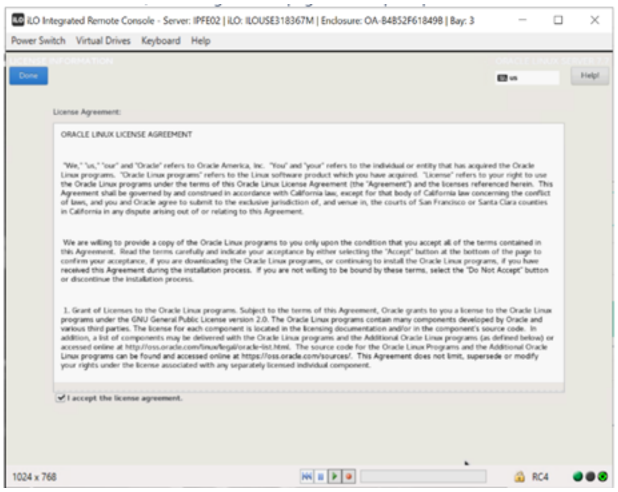
Oracle Linux is now successfully installed and ready for you to use!
Go ahead and reboot to start using it!

Use of this product is subject to the license agreement found at /usr/share/oraclelinux-release/EULA

10. To reboot host after the installation is completed, click **Reboot**.

    After reboot is done, license agreement page appears.

Figure 2-66 License Agreement


iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F618498 | Bay: 3
Power Switch
Virtual Drives
Keyboard
Help
LICENSE INFORMATION
ORACLE LINUX SERVER 7.7
Done
us
Help!
1024 x 768
RC4

License Agreement:

ORACLE LINUX LICENSE AGREEMENT

"We," "us," "our" and "Oracle" refers to Oracle America, Inc. "You" and "your" refers to the individual or entity that has acquired the Oracle Linux programs. "Oracle Linux programs" refers to the Linux software product which you have acquired. "License" refers to your right to use the Oracle Linux programs under the terms of this Oracle Linux License Agreement (the "Agreement") and the licenses referenced herein. This Agreement shall be governed by and construed in accordance with California law, except for that body of California law concerning the conflict of laws, and you and Oracle agree to submit to the exclusive jurisdiction of, and venue in, the courts of San Francisco or Santa Clara counties in California in any dispute arising out of or relating to this Agreement.

We are willing to provide a copy of the Oracle Linux programs to you only upon the condition that you accept all of the terms contained in this Agreement. Read the terms carefully and indicate your acceptance by either selecting the "Accept" button at the bottom of the page to confirm your acceptance, if you are downloading the Oracle Linux programs, or continuing to install the Oracle Linux programs, if you have received this Agreement during the installation process. If you are not willing to be bound by these terms, select the "Do Not Accept" button or discontinue the installation process.

1. Grant of Licenses to the Oracle Linux programs. Subject to the terms of this Agreement, Oracle grants to you a license to the Oracle Linux programs under the GNU General Public License version 2.0. The Oracle Linux programs contain many components developed by Oracle and various third parties. The license for each component is located in the licensing documentation and/or in the component's source code. In addition, a list of components may be delivered with the Oracle Linux programs and the Additional Oracle Linux programs (as defined below) or accessed online at http://oss.oracle.com/linux/legal/oracle-list.html. The source code for the Oracle Linux Programs and the Additional Oracle Linux programs can be found and accessed online at https://oss.oracle.com/sources/. This Agreement does not limit, supersede or modify your rights under the license associated with any separately licensed individual component.

☑ I accept the license agreement.

11. To accept license agreement, read and check **I accept the license agreement** checkbox, and click **Done** to continue.

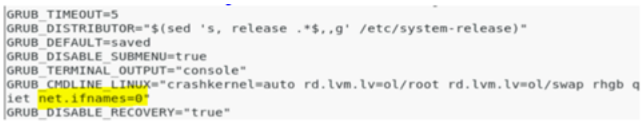
    > ⓘ **Note**
    >
    > Skip when prompted for ULN settings.

12. Login, select Language, and click **Next**.
13. Select Keyboard layout and click **Next**.
14. Turn off the location services and click **Next**.
15. Click **Skip** when prompted to connect to online accounts.
16. To verify kernel and KVM versions, open **SSH Console** window and check the following.

- # sudo su –
- # virt -manager
- # uname -a
- o # virsh version

17. To change network interface name pattern to **ethx**, perform the following steps:
    a. To append `'net.ifnames=0'` with option `GRUB_CMDLINE_LINUX`, edit `/etc/default/grub`

    ```
    cat /etc/default/grub
    ```

    ```
    GRUB_TIMEOUT=5
    GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
    GRUB_DEFAULT=saved
    GRUB_DISABLE_SUBMENU=true
    GRUB_TERMINAL_OUTPUT="console"
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb q
    iet net.ifnames=0"
    GRUB_DISABLE_RECOVERY="true"
    ```

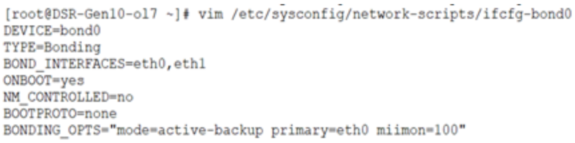
    b. Re-create the grub2 config file.

    ```
    grub2-mkconfig -o /boot/grub2/grub.cfg
    ```

    c. Restart host and verify that the network interfaces have **ethx** name pattern.

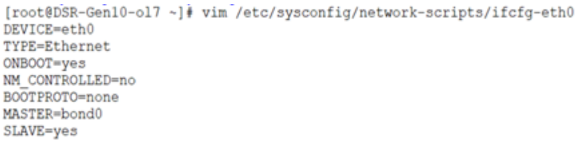
    ```
    shutdown -r
    ```

18. To create bond0 device, perform the following steps:
    a. Create device bond0 configuration file, save the file and exit.

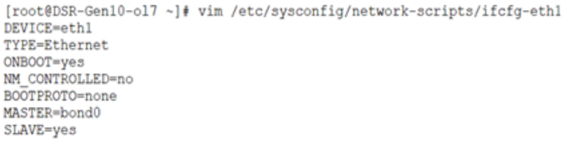
    ```
    [root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-bond0
    DEVICE=bond0
    TYPE=Bonding
    BOND_INTERFACES=eth0,eth1
    ONBOOT=yes
    NM_CONTROLLED=no
    BOOTPROTO=none
    BONDING_OPTS="mode=active-backup primary=eth0 miimon=100"
    ```

    b. Create device eth0 configuration file, save the file and exit.

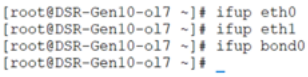
    ```
    [root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
    DEVICE=eth0
    TYPE=Ethernet
    ONBOOT=yes
    NM_CONTROLLED=no
    BOOTPROTO=none
    MASTER=bond0
    SLAVE=yes
    ```

    c. Create device eth1 configuration file, save the file and exit.

    ```
    [root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth1
    DEVICE=eth1
    TYPE=Ethernet
    ONBOOT=yes
    NM_CONTROLLED=no
    BOOTPROTO=none
    MASTER=bond0
    SLAVE=yes
    ```

    d. Bring up devices into services.

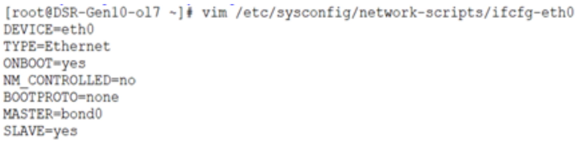


```
[root@DSR-Gen10-ol7 ~]# ifup eth0
[root@DSR-Gen10-ol7 ~]# ifup eth1
[root@DSR-Gen10-ol7 ~]# ifup bond0
[root@DSR-Gen10-ol7 ~]# _
```

19. To create IMI bridge, perform the following steps:

    a. Create `bond0.<imi_vlan>` configuration file.

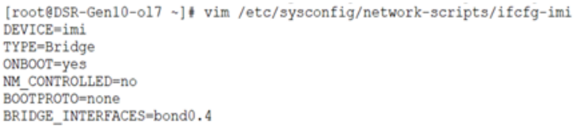
       ```
       vim /etc/sysconfig/network-scripts/ifcfg-bond0.<imi_vlan>
       ```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
```

    b. Create imi device configuration file.

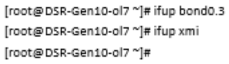
       ```
       vim /etc/sysconfig/network-scripts/ifcfg-imi
       ```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-imi
DEVICE=imi
TYPE=Bridge
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BRIDGE_INTERFACES=bond0.4
```

    c. Bring up devices into services.

Figure 2-67 Devices

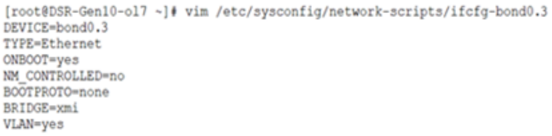


```
[root@DSR-Gen10-ol7 ~]# ifup bond0.3
[root@DSR-Gen10-ol7 ~]# ifup xmi
[root@DSR-Gen10-ol7 ~]#
```

20. To create XMI bridge, perform the following steps:

    a. Create `bond0.<xmi_vlan>` configuration file.

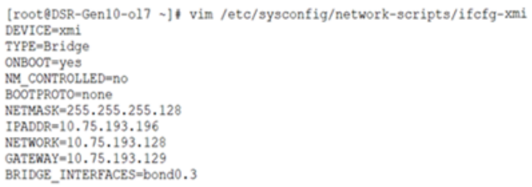
       ```
       vim /etc/sysconfig/network-scripts/ifcfg-bond0.<xmi_vlan>
       ```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-bond0.3
DEVICE=bond0.3
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BRIDGE=xmi
VLAN=yes
```

    b. Create xmi device configuration file.

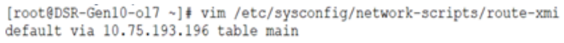
       ```
       vim /etc/sysconfig/network-scripts/ifcfg-xmi
       ```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-xmi
DEVICE=xmi
TYPE=Bridge
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
NETMASK=255.255.255.128
IPADDR=10.75.193.196
NETWORK=10.75.193.128
GATEWAY=10.75.193.129
BRIDGE_INTERFACES=bond0.3
```

c. Set default route for xmi network.

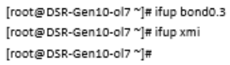
```
vim /etc/sysconfig/network-scripts/route-xmi default via <xmi_gateway>
table main
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/route-xmi
default via 10.75.193.196 table main
```

d. Bring up the devices into service.

Figure 2-68 Devices

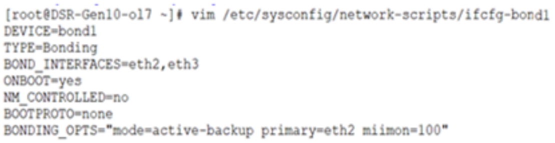


```
[root@DSR-Gen10-ol7 ~]# ifup bond0.3
[root@DSR-Gen10-ol7 ~]# ifup xmi
[root@DSR-Gen10-ol7 ~]#
```

21. To create bond1 device, perform the following steps:

a. Create device bond1 configuration file.

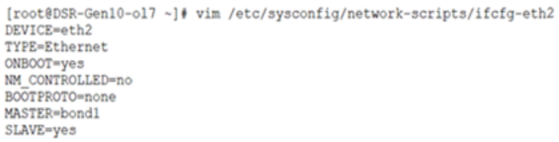
```
vim /etc/sysconfig/network-scripts/ifcfg-bond1
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-bond1
DEVICE=bond1
TYPE=Bonding
BOND_INTERFACES=eth2,eth3
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BONDING_OPTS="mode=active-backup primary=eth2 miimon=100"
```

b. Create device eth2 configuration file.

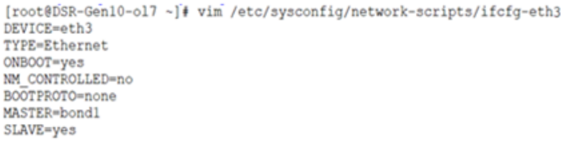
```
vim /etc/sysconfig/network-scripts/ifcfg-eth2
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth2
DEVICE=eth2
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MASTER=bond1
SLAVE=yes
```

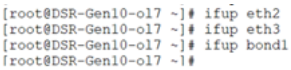
c. Create device eth3 configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-eth3
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth3
DEVICE=eth3
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MASTER=bond1
SLAVE=yes
```

d. Bring up devices into services.

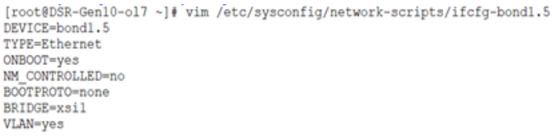


```
[root@DSR-Gen10-ol7 ~]# ifup eth2
[root@DSR-Gen10-ol7 ~]# ifup eth3
[root@DSR-Gen10-ol7 ~]# ifup bond1
[root@DSR-Gen10-ol7 ~]#
```

22. To create xsi1/xsi2 bridge, perform the following steps:

a. Create device `bond1.<xsi1_vlan>` configuration file.

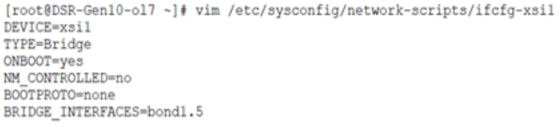
```
vim /etc/sysconfig/network-scripts/ifcfg-bond1.<xsi1_vlan>
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-bond1.5
DEVICE=bond1.5
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BRIDGE=xsi1
VLAN=yes
```

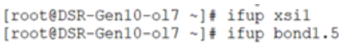
b. Create device xsi1 configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-xsi1
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-xsi1
DEVICE=xsi1
TYPE=Bridge
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BRIDGE_INTERFACES=bond1.5
```

c. Bring up devices into services.



```
[root@DSR-Gen10-ol7 ~]# ifup xsi1
[root@DSR-Gen10-ol7 ~]# ifup bond1.5
```

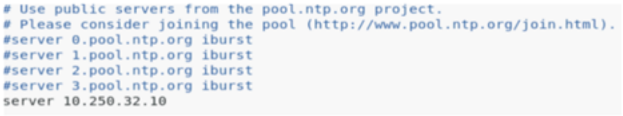
> **Note**
>
> Perform similar steps to create network devices for xsi2.

23. To set hostname, rename host by modifying `/etc/hostname` file.

```
# cat /etc/hostname
# vim /etc/hostname
    - Review the hostname
# hostnamectl status
```

24. To set NTP service, perform the following steps:

a. Modify `/etc/chrony.conf` configuration file. Then, comment out all server `*` entries and append your NTP server IP to the list with prepending 'server' text.

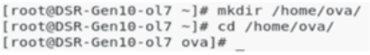


```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.pool.ntp.org iburst
#server 1.pool.ntp.org iburst
#server 2.pool.ntp.org iburst
#server 3.pool.ntp.org iburst
server 10.250.32.10
```

b. Force ntp to sync with newly added server.

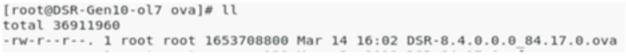
```
$ chronyc ntpdata <Remote ip address>
$ timedatectl
$ chronyc tracking
```

25. To create `/home/ova` directory, run the following command.



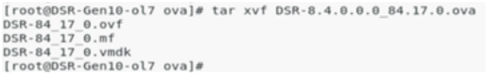
```
[root@DSR-Gen10-ol7 ~]# mkdir /home/ova/
[root@DSR-Gen10-ol7 ~]# cd /home/ova/
[root@DSR-Gen10-ol7 ova]# _
```

26. To transfer OVA file directory, use sftp tool.



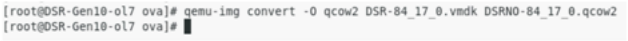
```
[root@DSR-Gen10-ol7 ova]# ll
total 36911960
-rw-r--r--. 1 root root 1653708800 Mar 14 16:02 DSR-8.4.0.0.0_84.17.0.ova
```

27. To untar the ova file, run the following command.



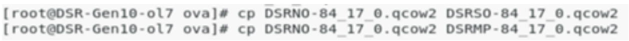
```
[root@DSR-Gen10-ol7 ova]# tar xvf DSR-8.4.0.0.0_84.17.0.ova
DSR-84_17_0.ovf
DSR-84_17_0.mf
DSR-84_17_0.vmdk
[root@DSR-Gen10-ol7 ova]#
```

28. To convert the `vmdk` file to `qcow2` file, run the following command.



```
[root@DSR-Gen10-ol7 ova]# qemu-img convert -O qcow2 DSR-84_17_0.vmdk DSRNO-84_17_0.qcow2
[root@DSR-Gen10-ol7 ova]#
```

29. To copy the `qcow2` files for **SO** and **MP**, run the following command.



```
[root@DSR-Gen10-ol7 ova]# cp DSRNO-84_17_0.qcow2 DSRSO-84_17_0.qcow2
[root@DSR-Gen10-ol7 ova]# cp DSRNO-84_17_0.qcow2 DSRMP-84_17_0.qcow2
```

30. To configure storage for corresponding `qcow2` files as per VMs, perform the following steps:

a. Set the storage for each VM by running the following command:

```
qemu-img resize <NO_qcow2_filename>.qcow2 <storage_in_gigabytes>G
```

b. Run the command for a VM if storage required is greater than 60 G.

For example: If resource profile is 2K Sh and VM is NOAMP,whereas the storage required is 120G, then run the following command:

```
qemu-img resize DSRNO-84_17_0.qcow2 70G
```

> **Note**
>
> - No need to run this command if the storage required is less than or equal to 60G.
> - For multiqueue settings, refer to Multiqueue on IPFE (KVM).

31. To set the txqueue length for the ether-net adapter to a high value on the host machine, add the following script to the created file `/sbin/ifup-local`.

```
[root@DSR-Gen10-ol7 ova]# vim /sbin/ifup-local
ifconfig eth0 txqueuelen 120000
ifconfig eth1 txqueuelen 120000
ifconfig eth2 txqueuelen 120000
ifconfig eth3 txqueuelen 120000
```

32. To verify txqueue length for the ether-net adapter to a high value on the host machine that is added on all interfaces, run the following command.

```
[root@DSR-Gen10-ol7 ova]# ifconfig <ethernet adapter>
```

> **Note**
>
> Verify same for eth1, eth2, and eth3.

33. To restart all the ethernet adapters (eth0, eth1, eth2, and eth3), run the following command on each adapter one at a time.

```
[root@DSR-Gen10-ol7 ova]# ifdown <ethernet adapter>
[root@DSR-Gen10-ol7 ova]# ifup <ethernet adapter>
```

34. Perform the listed steps in the Ring Buffer and txqueuelen Configuration (KVM) OL8.9 section.
35. To reboot the host machine, run the following command.

```
[root@DSR-Gen10-ol7 ova]# reboot
```

36. To confirm the configurations, verify the following on host machine as per the configuration:
    - The multiqueue configuration is performed on IPFE, ensure the configuration is done as mentioned in Multiqueue on IPFE (KVM).
    - The ring buffer size must be set to max on all the ether-net devices by using the steps in the Ring Buffer and txqueuelen Configuration (KVM) OL8.9 section.
    - The `txqueue` length for all the ether-net adapter must be set to a high value as stated in Step 31.

2.5.2 Creating and Installing OCDSR VMs through KVM GUI

This procedure installs DSR VMs NO, SO, and MP using KVM GUI.

> **Note**
>
> This installation procedure is only applicable for each VM, that is NO, SO, MP and so on.

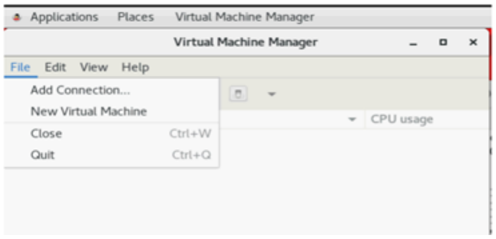
Prerequisites:

- Installation of DSR on Oracle Linux OS through KVM must be performed.

1. To log in to the host machine and open the Virual Machine, run the following command:

   ```
   virt-manager
   ```

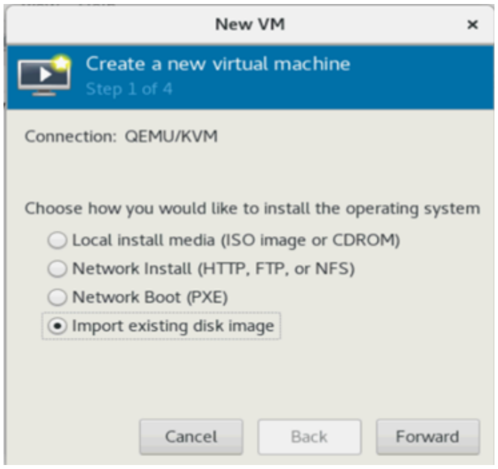
   Figure 2-69   Virtual Machine Manager

   > **Note**
   >
   > Ensure X11 forwarding is enabled before running `virt-manager` command on CLI.

2. To create a new Virtual Machine, on Virtual Manager GUI, click **File**, and then **New Virtual Machine** and select **Import existing disk image**.

   Figure 2-70   Creating a New VM

   New VM

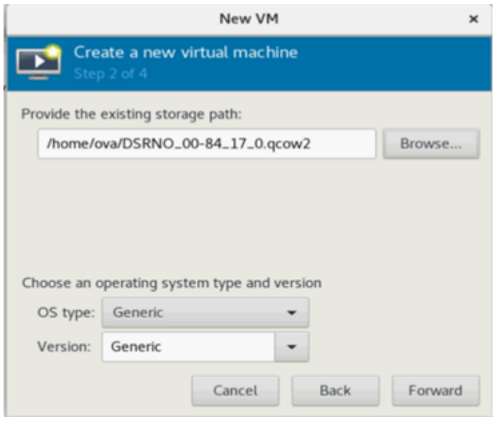
   Create a new virtual machine
   Step 1 of 4

   Connection: QEMU/KVM

   Choose how you would like to install the operating system

   ○ Local install media (ISO image or CDROM)
   ○ Network Install (HTTP, FTP, or NFS)
   ○ Network Boot (PXE)
   ● Import existing disk image

3. To select the image file, select the qcow2 image by browsing the `/home/ova` location and click **Forward**.



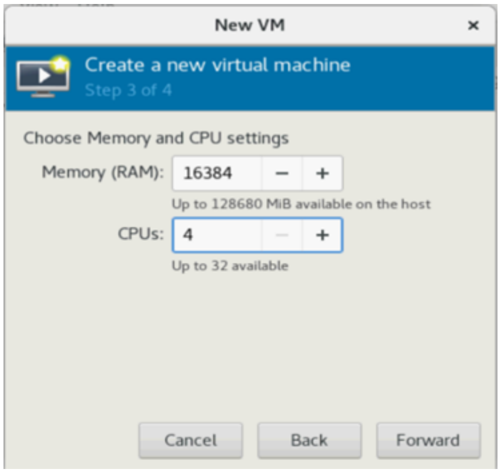
Create a new virtual machine
Step 2 of 4

Provide the existing storage path:
/home/ova/DSRNO_00-84_17_0.qcow2

Choose an operating system type and version
OS type: Generic
Version: Generic

> **Note**
>
> Refer to Install DSR on Oracle Linux/KVM section.

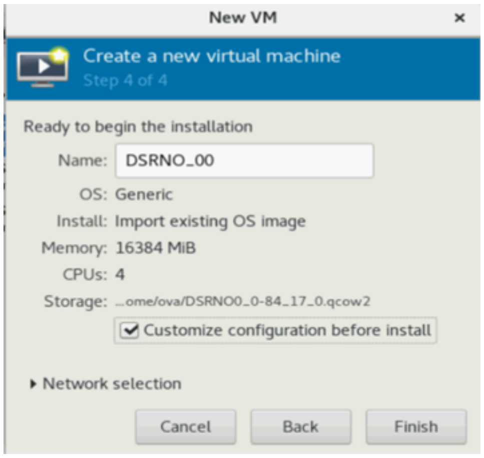
4. For each VM, select the RAM and vCPUs as required by resource profile and click **Forward**.



Create a new virtual machine
Step 3 of 4

Choose Memory and CPU settings
Memory (RAM): 16384
Up to 128680 MiB available on the host
CPUs: 4
Up to 32 available

5. To verify and customize VM, perform the following steps:.
   1. Update the VM name and select **Customize configuration before install**.
   2. Select **XMI bridge** under **Network** selection and click **Finish**.



Ready to begin the installation

Name: DSRNO_00

OS: Generic

Install: Import existing OS image

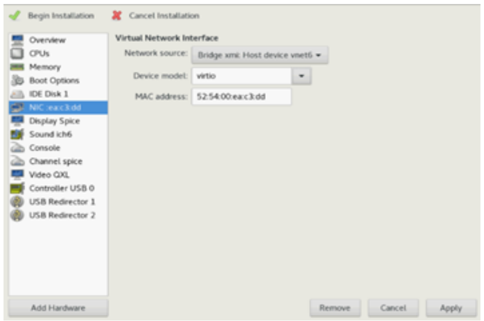
Memory: 16384 MiB

CPUs: 4

Storage: ...ome/ova/DSRNO0_0-84_17_0.qcow2

☑ Customize configuration before install

6. For XMI bridge, modify the Device model to virtio.



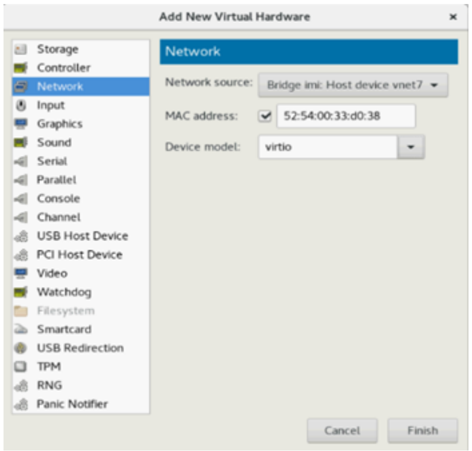
Virtual Network Interface

Network source: Bridge xmi: Host device vnet6

Device model: virtio

MAC address: 52:54:00:ea:c3:dd

7. To customize the network configuration, perform the following steps:
   a. On the next screen, click **Add Hardware** and configure as following:
      - Under **Network** source, choose **IMI Bridge**.
      - For NO and SO, choose IMI bridge only.
      - For MP, add XSI1, along with IMI by repeating this step.



Network

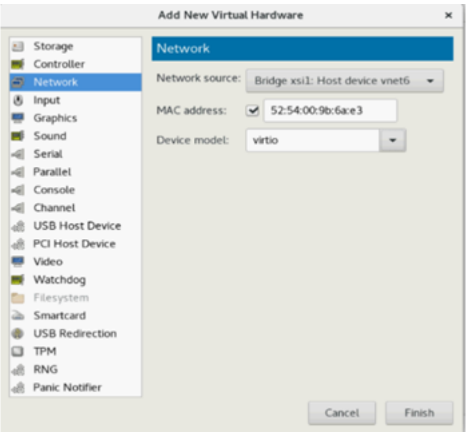
Network source: Bridge imi: Host device vnet7

MAC address: ☑ 52:54:00:33:d0:38

Device model: virtio

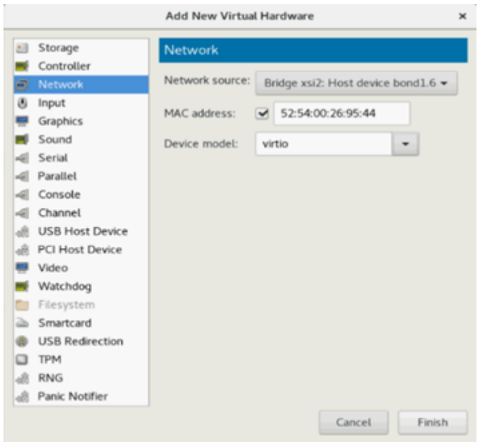
   b. Click **Finish**.

c. For MP, add XSI1 and XSI2 bridge.
For XSI1 bridge:



Network source: Bridge xsi1: Host device vnet6
MAC address: ☑ 52:54:00:9b:6ace3
Device model: virtio

For XSI2 bridge:



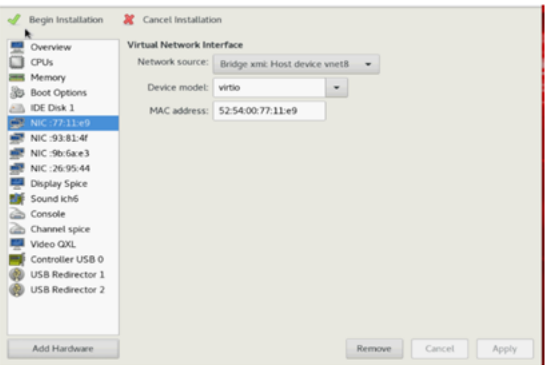
Network source: Bridge xsi2: Host device bond1.6
MAC address: ☑ 52:54:00:26:95:44
Device model: virtio

> **Note**
>
> For DSR Topology it is recommended to add all interfaces on each VM, even when the VM does not require that interface or does not use a VLAN.
> This is to use a standard when the topology is created from NOAM GUI.

DSR VMs	
XMI	eth0
IMI	eth1
XSI1	eth2
XSI2	eth3

Add all interfaces as needed. Once the other networks are added, the NICs appears.

8. After adding all bridges, verify and begin the VM installation.



Virtual Network Interface

Network source: Bridge xml: Host device vnet8

Device model: virtio

MAC address: 52:54:00:77:11:e9

9. To disable the TSO GSO features for SBR server, see Disabling TSO GSO features for SBR server.

2.6 Optional Features

Once DSR installation is complete, perform the configuration and installation for optional features that may be present in this deployment. Refer to the following table for the post-DSR installation configuration documentation needed for their components.

Table 2-4 Post-DSR Installation Configuration Step

Feature	Document
Diameter Mediation	*DSR Meta Administration Feature Activation Procedure*
Full Address Based Resolution (FABR)	*DSR FABR Feature Activation Procedure*
Range Based Address Resolution (RBAR)	*DSR RBAR Feature Activation Procedure*
SCEF Feature Activation	*DSR SCEF Feature Activation Guide*
Policy and Charging Application (PCA)	*PCA Activation Procedure*
Host Intrusion Detection System (HIDS)	*DSR Security Guide, Section 3.2*
Diameter Custom Applications (DCA)	*DCA Framework and Application Activation and Deactivation Procedures*

3

Software Installation Procedure

The host and virtual networks configuration should be done before running the procedures in this document. It is assumed that at this point the user has access to the following:

- 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 OVAs 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 accessible

SUDO

Many commands when run as admusr (non-root user) requires 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 is introduced in DSR. Standard IPv6 formats for IPv6 and prefix can be used in all IP configuration screens, which enables the DSR to run in an IPv6 only environment. When using IPv6 for XMI and management, place the IPv6 address in brackets.

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

If a dual-stack (IPv4 and IPv6) network is required, configure the topology with IPv4 first, and then migrate to IPv6. Refer to *DSR IPv6 Migration Guide* for instructions on this migration.

3.1 Creating DSR Guests (VMware)

Perform the following tasks to create DSR guests for VMware.

3.1.1 Importing DSR OVA (VMware)

This procedure adds the DSR OVA to the VMware catalog or repository.

1. Launch the required VMware client.
2. Add the DSR OVA image to the VMware catalog or repository.

> **Note**
>
> Refer to the instructions provided by the Cloud solutions manufacturer.

3.1.2 Configuring NOAM Guests Role Based On Resource Profile and Configure Network (VMware)

This procedure configures networking on VMs.

1. To create the NOAM1 VM from the OVA image, perform the following steps:
   1. Browse to the library or repository where the **OVA** image is placed.
   2. Deploy the OVA Image by using **vSphere Client** or **vSphere Web Client**.
   3. Name the **NOAM1 VM** and select the data store.
2. Configure resources for the NOAM1 VM using the **vSphere Client** or **vSphere Web Client**, by referring to the *DSR Cloud Benchmarking Guide* for the required DSR NOAM resource profile.
3. To power ON NOAM1, use the **vSphere Client** or **vSphere Web Client**.
4. To configure NOAM1, perform the following steps:
   1. Access the **NOAM1 VM** console through the **vSphere Client** or **vSphere Web Client**.
   2. Login as the **admusr** user.
   3. Set the <ethX> device.

      ```
      $ sudo netAdm add --device=<ethX> --address=<IP Address in External
      management Network> --netmask=<Netmask> --onboot=yes --bootproto=none
      ```

      > **Note**
      >
      > Here, ethX is the interface associated with the XMI network.

   4. Add the default route for ethX.

      ```
      $ sudo netAdm add --route=default --gateway=<gateway address for the
      External management network> --device=<ethX>
      ```

   5. Ping the XMI gateway for network verification.

      ```
      $ ping –c3 <Gateway of External Management Network>
      ```

> **Note**
>
> To configure NOAM2, repeat the above 4 steps.

3.1.3 Configure Remaining DSR Guests Based on Resource Profile and Configure Network

This procedure adds network addresses for all VMs.

> **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.

1. Create the SOAM1 VM from the OVA image.
   a. Browse to the library or repository where the **OVA** image is placed.
   b. Deploy the OVA Image by using **vSphere Client** or **vSphere Web Client**.
   c. Name the **SOAM1 VM** and select the data store.
2. Configure the SOAM1 VM as per the resource profiles defined in *DSR Cloud Benchmarking Guide* for the **DSR SO** using the **vSphere Client** or **vSphere Web Client**. Interfaces must be added per the OCDSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.
3. Power ON SOAM1 VM.
   a. Power ON the **DSR SOAM1 VM** with the **vSphere Client** or **vSphere Web Client**.
   b. Monitor the vApps screen's Virtual Machines tab until the DSR VM reports **Powered On** in the Status column.
4. Configure XMI interface.
   a. Access the **VM console** through the **vSphere Client** or **vSphere Web Client**.
   b. Login as the **admusr** user.
   c. Set the ethX device:

```
$ sudo netAdm add --device=<ethX> --address=<IP Address in External
Management Network> --netmask=<Netmask> --onboot=yes --bootproto=none
```

> **Note**
>
> Where ethX is the interface associated with the XMI network.

   d. Add the default route for ethX:

```
$ sudo netAdm add --route=default --gateway=<gateway address for the
External management network> --device=<ethX>
```

5. Verify network connectivity.
   a. Access the **SOAM1 VM console** using the **vSphere Client** or **vSphere Web Client**.
   b. Login as the **admusr** user.

c. Ping the NOAM1.

```
$ ping -c3 <IP Address in External Management Network>
```

> **Note**
>
> Repeat the above procedure for the following VMs. Use unique labels for the VM names:
>
> - MP(s)
> - IPFE(s)
> - SOAM(s)
> - Session SBRs, Binding SBR (Optional Components)
> - DR NOAMs (Optional Components)

3.2 Create DSR Guests (KVM/OpenStack)

Perform the following tasks to create DSR guests in KVM or OpenStack.

3.2.1 Import DSR OVA (KVM/OpenStack Only)

This procedure adds the DSR image to the glance image catalog.

Prerequisites:

- Create instance flavors.
  If not yet done, use the resource profiles defined in *DSR Cloud Benchmarking Guide* values to create flavors for each type of VM. Flavors can be created with the Horizon GUI in the **Admin** section, or with the nova flavor-create command line tool. Make the flavor names as informative as possible. As flavors describe resource sizing, a common convention is to use a name like “0406060” where the first two figures (04) represent the number of virtual CPUs, the next two figures (06) might represent the RAM allocation in GB and the final three figures (060) might represent the disk space in GB.
- If using an Intel 10 Gigabit Ethernet ixgbe driver on the host nodes, note that the default LRO (Large Receive Offload) option must be disabled on the host command line. Refer to the *Intel Release Notes* for more details. This action can be performed using the following command.

  ```
  $ sudo ethtool -K <ETH_DEV> lro off
  ```

- If using IPFE Target Set Addresses (TSA):
  - Read and understand the "Disable Port Security" procedure in Disable Port Security, including the warning note.
  - Enable the Neutron port security extension.

> **Note**
>
> - This step is not applicable for HEAT deployment.
> - If the DSR guest type is IPFE, see Performance Tuning Recommended .

To add DSR OVA image perform the following steps:

1. Copy the OVA file to the OpenStack control node.

   ```
   $ scp DSR-x.x.x.x.x.x.ova admusr@node:~
   ```

2. Log in to the OpenStack control node.

   ```
   $ ssh admusr@node
   ```

3. In an empty directory, unpack the OVA file using **tar**.

   ```
   $ tar xvf DSR-x.x.x.x.x.x.ova
   ```

4. One of the unpacked files has a **.vmdk** suffix. This is the VM image file that must be imported.
   `DSR-x.x.x.x.x-disk1.vmdk`
5. Source the OpenStack **admin** user credentials.

   ```
   $ .  keystonerc_admin
   ```

6. Select an informative name for the new image.

   ```
   dsr-8.6.x.x.x-original
   ```

7. Import the image using the **glance** utility from the command line.

   ```
   $ glance image-create --name dsr-x.x.x.x-original --visibility private --
   protected false --progress --container-format bare --disk-format vmdk --
   file DSR-x.x.x.x-disk1.vmdk
   ```

   This process takes about 5 minutes depending on the underlying infrastructure.
8. Convert VMDK to QCOW2 format.
   Use the **qemu-img** tool to create a qcow2 image file using this command.

   ```
   qemu-img convert -f vmdk -O qcow2 <VMDK filename> <QCOW2 filename>
   ```

   Example:

   ```
   qemu-img convert -f vmdk -O qcow2 DSR-82_12_0.vmdk DSR-82_12_0.qcow2
   ```

   Install the qemu-img tool (if not already installed) using this yum command.

   ```
   sudo yum install qemu-img
   ```

9. Import the converted qcow2 image using the “glance” utility from the command line.

   ```
   $ glance image-create --name dsr-x.x.x-original --is-public True --is-
   protected False --progress  --container-format bare --disk-format qcow2 --
   file DSR-x.x.x-disk1.qcow2
   ```

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

   > **Note**
   >
   > The above two steps (8 and 9) are optional and are not needed if VMDK is used.

3.2.2 Configure NOAM Guests Role Based on Resource Profile (KVM/ OpenStack Only)

This procedure configures networking on VMs.

1. Name the new VM instance.
   a. Create an informative name for the new instance: NOAM1.
   b. Examine the DSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.
2. Create and boot the NOAM VM instance from the glance image.
   a. Get the following configuration values.
      The image ID

      ```
      $ glance image-list
      ```

      The flavor ID

      ```
      $ nova flavor-list
      ```

      The network ID (s)

      ```
      $ neutron net-list
      ```

      An informative name for the instance:

      - NOAM1
      - NOAM2

   b. 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 DSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.

> **Note**
>
> IPv6 addresses should use the **v6-fixed-ip** argument instead of **v4-fixed-ip**.
>
> ```
> $ nova boot --image <image ID> --flavor <flavor id> --nic net-
> id=<first network id>,v4-fixed-ip=<first ip address> --nic net-
> id=<second network id>,v4-fixed-ip=<second ip address> <instance
> name>
> ```

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

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

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

3. Configure NOAM VIP.

   This is an optional step.

   > **Note**
   >
   > For information about Firewall Ports, refer to *DSR IP Flow* document. Refer to Application VIP Failover Options (OpenStack) for more information on VIP.

   If a NOAM VIP is needed, run the following commands:

   a. Find the port ID associated with the NOAM instance XMI interface.

   ```
   $ neutron port-list
   ```

   b. Add the VIP IP address to the address pairs list of the NOAM instance XMI interface port.

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

4. Check if interface is configured.

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

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

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

5. Manually configure interface, if not already done.

   This is an optional step.

> **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.

a. Log in to the **Horizon** GUI as the DSR tenant user.

b. Go to the **Compute/Instances** section.

c. Click the **Name** field of the newly created instance.

d. Select the **Console** tab.

e. Log in as the `admusr` user.

f. Configure the network interfaces, conforming with the DSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.

```
$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --
netmask=<xmi net mask>
$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway
ip>
```

Verify network connectivity by pinging Gateway of XMI network.

```
$ ping –c3 <XMI Gateway>
```

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

g. Reboot the NOAM VM. It takes approximately 5 minutes for the VM to complete rebooting.

```
$ sudo init 6
```

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

> **Note**
>
> To configure NOAM2, repeat the above steps for NOAM2.

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

This procedure adds network addresses for all VMs.

> **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.

1. Name the new VM instance.
   a. Create an informative name for the new instance: **SOAM1**.
   b. Examine the DSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.
2. Create and boot the SOAM VM instance from the glance image.
   a. Get the following configuration values.
      The image ID

      ```
      $ glance image-list
      ```

      The flavor ID

      ```
      $ nova flavor-list
      ```

      The network ID(s)

      ```
      $ neutron net-list
      ```

      An informative name for the instance:

      - SOAM1
      - SOAM2
   b. 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 DSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.

      > **Note**
      >
      > IPv6 addresses should use the **v6-fixed-ip** argument instead of **v4-fixed-ip**.
      >
      > ```
      > $ nova boot --image <image ID> --flavor <flavor id> --nic net-
      > id=<first network id>,v4-fixed-ip=<first ip address> --nic net-
      > id=<second network id>,v4-fixed-ip=<second ip address> <instance
      > name>
      > ```

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

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

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

   This is an optional step.

> **Note**
>
> Refer to Allowed Address Pairs for more information on VIP.

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

a. Find the port ID associated with the SOAM instance XMI interface.

```
$ neutron port-list
```

b. Add the VIP IP address to the address pairs list of the SOAM instance XMI interface port.

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

4. Check if interface is configured.

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

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

   If the ping is successful, ignore step 5.

5. Manually configure interface, if not already done.

   This is an optional step.

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

a. Log in to the **Horizon** GU I as the DSR tenant user.

b. Go to the **Compute/Instances** section.

c. Click the **Name** field of the newly created instance.

d. Select the **Console** tab.

e. Log in as the **admusr** user.

f. Configure the network interfaces, conforming with the DSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.

```
$ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --
netmask=<xmi net mask>

$ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway
ip>
```

Verify network connectivity by pinging Gateway of XMI network.

```
$ ping -c3 <XMI Gateway>
```

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

6. Reboot the SOAM VM. It takes approximately 5 minutes for the VM to complete rebooting.

   ```
   $ sudo init 6
   ```

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

7. Verify network connectivity.
   a. Access the **SOAM1 VM console** using OpenStack.
   b. Log in as the **admusr** user.
   c. Ping the NOAM1.

      ```
      $ ping -c3 <IP Address in External Management Network>
      ```

   Repeat above for the following VMs. Use unique labels for the VM names. Assign addresses to all desired network interfaces:

   - MP(s)
   - IPFE(s)
   - MP vSTP (For vSTP configuration) (Optional Components)
   - SOAM(s)
   - Session SBRs, Binding SBR (Optional Components)
   - DR NOAMs (Optional Components)

3.3 Create DSR Guests (OVM-S/OVM-M)

Perform the following task to create DSR guests in OVM-S or OVM-M.

Prerequisites:
This procedure requires values for these variables:

- <OVM-M IP> = IP address to access a sh prompt on the OVM server
- <URL to OVA> = Link to a source for downloading the product image (.ova)
- <MyRepository name> = Name of the repository in the OVM to hold the product image (.ova)

Running this procedure discovers and uses the values of these variables:

- <Virtual Appliance OVA ID>
- <OVA VM name_vm_vm>
- <OVM network id for (each subnet)>
- <OVM network name for (each subnet)>

This procedure imports the DSR image.

1. Access command line of OVM.

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

   a. Get the site-specific values for these variables (overwrite example).
      `<OVM-M IP> = 100.64.62.221`

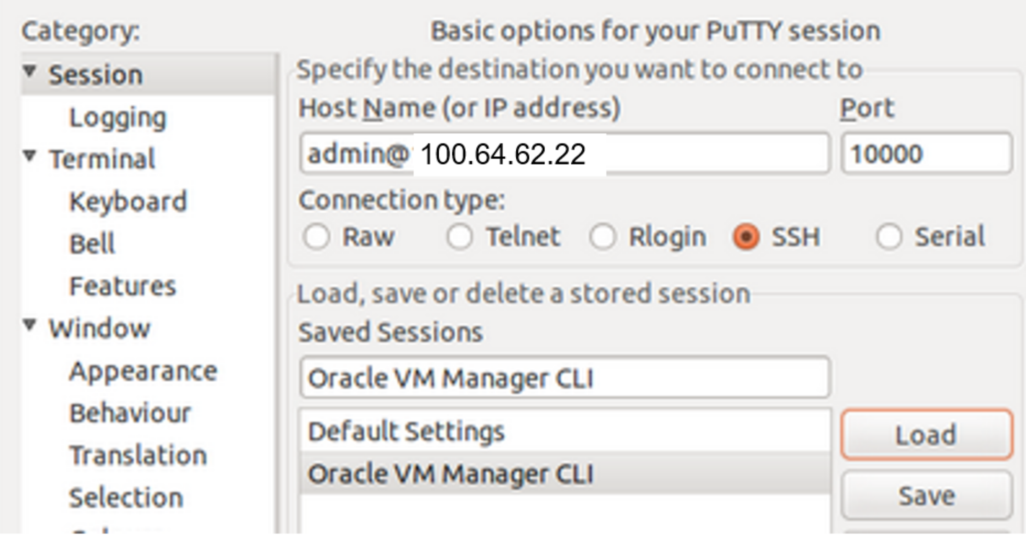
   b. Use the respective value for <OVM-M IP> into the command.

      ```
      ssh -l admin <OVM-M IP> -p 10000
      ```

      Example:

      ```
      ssl –l admin 100.64.62.221 –p 10000
      ```

      Alternatively, use a terminal emulation tool like putty.



Host Name (or IP address): admin@ 100.64.62.22

Port: 10000

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Saved Sessions: Oracle VM Manager CLI

2. In OVM-M CLI, import the VirtualAppliance/OVA.

   a. Get the site-specific values for these variables (overwrite example).
      <URL to OVA> = `http://10.240.155.70/iso/DSR/8.6/ova/DSR-9.2.0.0.0-102.16.0.ova`

      <MyRepository name> = `XLab Utility Repo01`

   b. Use the respective 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/8.6/ova/DSR-8.6.0.0.0_95.14.0.ova
      ```

   c. Run the command and validate success.

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

Command:

```
importVirtualAppliance Repository name='XLab Utility Repo01'
url=http://10.240.155.70/iso/DSR/8.6/ova/DSR-9.2.0.0.0-102.16.0.ova
Status: Success
Time: 2017-04-18 15:23:31,044 EDT
JobId: 1492543363365
Data:
id: 1128a1c6ce name: DSR-9.2.0.0.0-102.16.0.ova
```

e. Use the respective values for values for these variables (overwrite example).
<Virtual Appliance OVA ID> = `1128a1c6ce`

3. In OVM-M CLI, get the virtual appliance ID.

   The virtual appliance OVA ID is used in later steps.

   a. Get the site-specific text for these variables (overwrite example).
   <Virtual Appliance OVA ID> = `1128a1c6ce`

   b. Use the respective values for <Virtual Appliance OVA ID> into the command.

```
OVM> show VirtualAppliance id=<Virtual Appliance OVA id>
```

Example:

```
OVM> show VirtualAppliance id=1128a1c6ce
```

   c. Run the command and validate success.

   d. Examine the screen results to find site-specific text for variables in these locations.
   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/8.6/ova/DSR-9.0.2.0.0_95.14.0.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-9.2.0.0.0-102.16.0.ova]
Name = DSR-9.2.0.0.0-102.16.0.ova
Description = Import URL: http://10.240.155.70/iso/DSR/8.6/ova/
DSR-9.2.0.0.0-102.16.0.ova
Locked = false
```

   e. Use the respective values for these variables (overwrite example).
   <OVA VM name_vm_vm> = `11145510c0_vm_vm`

4. In OVM-M CLI, determine the OVM network IDs (established during the platform installation).

```
OVM> list Network
```

   a. Run the command and validate success.

   b. Examine the screen results to find the find site-specific OVM values for each subnet:

- <OVM network ID>
- <OVM network name>

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

```
Command: list network
Status: Success
Time: 2017-04-19 18:51:42,494 EDT
Data:  id:10486554b5  name:XSI-7 (10.196.237.0/25)
id:10f4d5744c  name:XMI-11 (10.75.159.0/25)
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
```

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

Table 3-1 Network ID Variables

	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

3.4 Configure Virtual Machines (OVM-S/OVM-M)

This procedure creates virtual machines. Repeat this procedure for each DSR VM guest that needs to be created.

Prerequisites:
This procedure requires values for these variables:

- <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

Running this procedure discovers and uses the values of these variables:

- <VM ID>
- <vCPUs Production>
- <VNIC 1 ID>
- <interface name> defined in *DSR Cloud Benchmarking Guide*

1. In OVM-M CLI, create a VM for each guest from the VM in the OVA virtual appliance.
   a. Get the site-specific text for these variables (overwrite example).
   <OVA VM name_vm_vm> = 11145510c0_vm_vm
   b. Use the respective values for <OVA VM name> in the command.

   ```
   OVM> createVmFromVirtualApplianceVm VirtualApplianceVm name=<OVA VM
   name>
   ```

   Example:

   ```
   OVM> createVmFromVirtualApplianceVm VirtualApplianceVm
   name=11145510c0_vm_vm
   ```

   c. Run the command and validate success.
   d. Examine the screen results to find site-specific text for variables in these locations.

   ```
   createVmFromVirtualApplianceVm VirtualApplianceVm name=11145510c0_vm_vm
   Status: Success
   Time: 2017-04-18 16:02:09,141 EDT
   JobId: 1492545641976
   Data:
   id: 0004fb00000600004a0e02bdf9fc1bcd
   name: DSR-9.2.0.0.0-102.16.0.ova_vm
   ```

   e. Use the respective values for these variables (overwrite example).
   <VM ID> = 0004fb00000600004a0e02bdf9fc1bcd
2. In OVM-M CLI, add the VM to the server pool.
   a. Get the site-specific text for these variables (overwrite example).
   <VM ID> = 0004fb00000600004a0e02bdf9fc1bcd

   <ServerPool name> = XLab Pool 01

   b. Use the respective values for <VM ID> and <ServerPool name> in 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"
   ```

   c. Run the command and validate success.

   ```
   add Vm id=0004fb0000060000beb93da703830d3c to ServerPool name="XLab
   Pool 01"
   ```

```
Status: Success
Time: 2017-04-19 21:05:10,950 EDT
JobId: 1492650310802
```

> **Note**
>
> Refer to Server Pool for more information.

3. In OVM-M CLI, edit VM to apply required profile or resources.
   a. Get the site-specific text for these variables (overwrite example).
   <VM ID> = 0004fb00000600004a0e02bdf9fc1bcd

   <VM name > = na-noam-na-2a

   <vCPUs Production> = 4
   b. Refer to *DSR Cloud Benchmarking Guide* for recommended resource.

Table 3-2 Recommended Resource

VM Name	vCPUs Lab	RAM (GB) Lab	vCPUs Production	RAM (GB) Production	Storage (GB) Lab and Production
Type of guest host	#	#	#	#	3

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

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

   Example:

```
OVM> edit Vm id=0004fb00000600004a0e02bdf9fc1bcd name=na-noam-na-2a
memory=6144 memoryLimit=6144 cpuCountLimit=4 cpuCount=4
domainType=XEN_HVM description="na-noam-na-2a"
```

   d. Run the command and validate success.

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

   Now, the VM has a name and resources.

4. In OVM-M CLI, determine VNIC ID.
   a. Get the site-specific text for these variables (overwrite example).
   <VM name> = na-noam-na-2a

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

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

Example:

```
OVM> show Vm name=na-noam-na-2a
```

c. Run the command and validate success.

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

```
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/9.0/ova/DSR-9.2.0.0.0-102.16.0.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
Locked = false
DeprecatedAttrs = [Huge Pages Enabled (Deprecated for PV guest)]
```

e. Use the respective values for these variables (overwrite example).
<Vnic 1 ID> = 0004fb0000070000091e1ab5ae291d8a

5. Determine network interfaces for the type of guest host.

   Refer to *DSR Cloud Benchmarking Guide* to learn which network interfaces need to be configured for each guest type. The following table provides details about the type of guest host:

Table 3-3 Network Interfaces

	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#

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

6. In OVM-M CLI, attach XMI VNIC (if required by guest host type).
   a. Get the site-specific text for these variables (overwrite example).
   <VNIC 1 ID> = 0004fb0000070000091e1ab5ae291d8a

   <OVM network ID for XMI> = 10345112c9

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

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

   Example:

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

   c. Run the following command and validate success.

   ```
   add Vnic id=0004fb0000070000091e1ab5ae291d8a to Network name=10345112c9
   Status: Success
   Time: 2017-04-19 19:08:59,496 EDT
   JobId: 1492643339327
   ```

7. In OVM-M CLI, create and attach IMI VNIC (if required by guest host type).
   a. Get the site-specific text for these variables (overwrite example).
   <VM name> = na-noam-na-2a

   <OVM network ID for IMI> = 102e89a481

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

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

   Example:

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

   c. Run 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. In OVM-M CLI, create and attach XSI VNIC(s) (if required by guest host type).

   > **Note**
   >
   > Repeat this step if the VM has multiple signaling networks, specifying the number of the network.

   a. Get the site-specific text for these variables (overwrite example).
      <VM name> = hostname

      <OVM network ID for XSI#> = 1053a604f0

      <#> = the number of the XSI network [1-16]

   b. Use the respective values for <OVM network ID for XSI#> and <VM name> into the command.

      ```
      OVM> create Vnic network=<OVM network id for XSI#> name=<VM name>-
      XSI<#> on Vm name=<VM name>
      ```

      Example:

      ```
      OVM> create Vnic network=1053a604f0 name=hostname-XSI1 on Vm
      name=hostname
      ```

   c. Run the command and validate success.

9. In OVM-M CLI, create and attach replication VNIC (if required by guest host type).

   a. Get the site-specific text for these variables (overwrite example).
      <VM name> = hostname

      <OVM network ID for Replication XSI#> = 10486554b5

      <OVM network name for Replication XSI#> = XSI7

      <#> = the number of the XSI Replication network [1-16]

   b. Use the respective values for <OVM network ID for Replication XSI#>, <OVM network name for Replication XSI#>, and <VM name> 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
```

c. Run the command and validate success.

10. In OVM-M CLI, start VM.

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

    ```
    <VM name> = na-noam-na-2a
    ```

    b. Use the respective values for <VM name> into the command.

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

    Example:

    ```
    OVM> start Vm name=na-noam-na-2a
    ```

    c. Run 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
    ```

11. In OVM-M GUI, configure the XMI network interface for this VM.

    a. Get the site-specific text for these variables (overwrite example).
    <URL for OVM GUI> = `https://100.64.62.221:7002/ovm/console/faces/resource/resourceView.jspx`

    <interface name> = from the table in *DSR Cloud Benchmarking Guide*

    <VM IP in XMI> = from the NAPD

    <Gateway for XMI> = from the NAPD

    <NetMask for XMI> = from the NAPD

    b. Access the CLI of the console for the VM.

    c. Log into the **OVM-M** GUI by typing the **<URL for OVM GUI>** into a browser.

       i. Navigate to the Servers and VMs tab.

       ii. Expand and select the <ServerPool name>.

       iii. From the **Perspective** list, select **Virtual Machines**.

       iv. Select the <VM name> from the rows listed, and click the **Launch Console** icon.

       v. In the Console window, log into the VM as the admusr.

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

XMI:

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

Example:

```
$ sudo netAdm set --onboot=yes --device=eth0 --address=10.75.158.189 --
netmask=255.255.255.128
```

Example:

```
$ sudo netAdm add --route=default --device=eth0 --gateway=10.75.158.129
```

e. Run the command and validate success.

f. Verify network connectivity by pinging Gateway of network.

```
$ ping –c3 <Gateway for XMI>
```

g. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.

```
$ sudo init 6
```

The new VM should now be accessible through both network and console.

3.5 DSR Installation of OL8 and KVM on X9

DSR Installation on OL8 and KVM includes the following procedures:

- Install DSR on Oracle Linux/KVM
- Create and install OCDSR VMs through KVM GUI

> **Note**
>
> If using a hardware in remote LAB then use a remote windows machine to install Linux. Ensure that OL8 ISO is also located locally in remote windows machine.

3.5.1 Install DSR on Oracle Linux/KVM

This procedure installs DSR configuration on Oracle Linux OS with direct KVM as hypervisor.

> **Note**
>
> - This installation procedure only applies when installing DSR on Oracle Linux OS via direct KVM.
> - For the Oracle Linux OS, Oracle Linux 8.x release is used and verified OK.
> - The snapshot used for this procedure has been taken from HP Gen-10 Blade.
> - This procedure can be run on any flavor of blade that requires DSR installation on OL8.x and KVM.

Prerequisites:
All the respective infrastructures has to be up and running.

Perform the following steps on each blade:

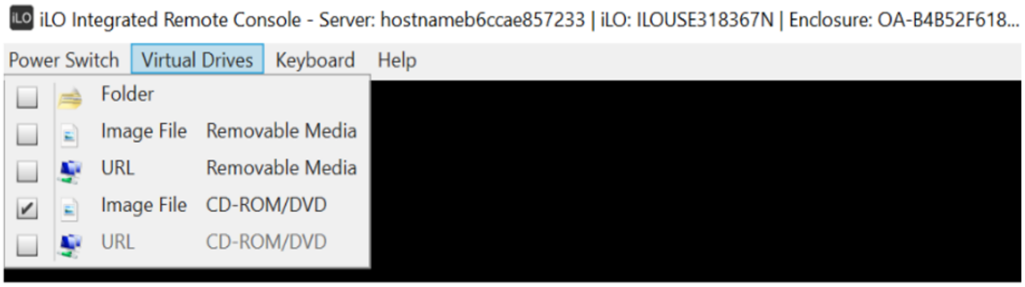
1. Mount virtual media contains Oracle Linux OS software.

   Follow steps defined in Mounting Virtual Media on Blade:

   - Open the ILO.
   - Attach the OEL 8.x ISO in ILOs virtual drives->Image File CD/DVD ROM.

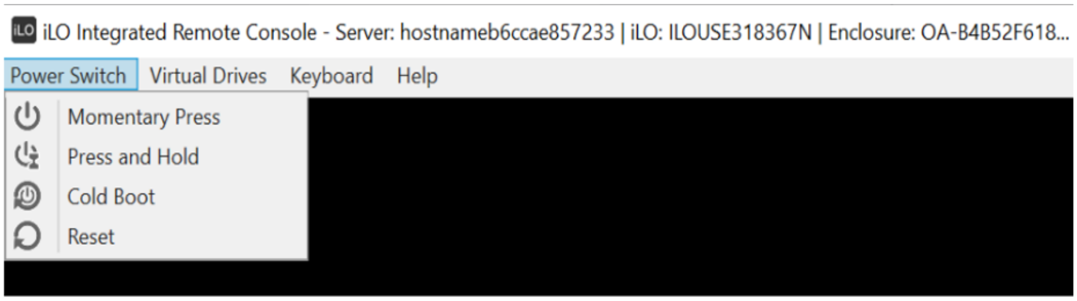
   To mount the Oracle Linux OS software ISO from ILO GUI:

   - Navigate to **Virtual drives**, and then **Menu**.
   - Click on **Image File**, then select image from folder.

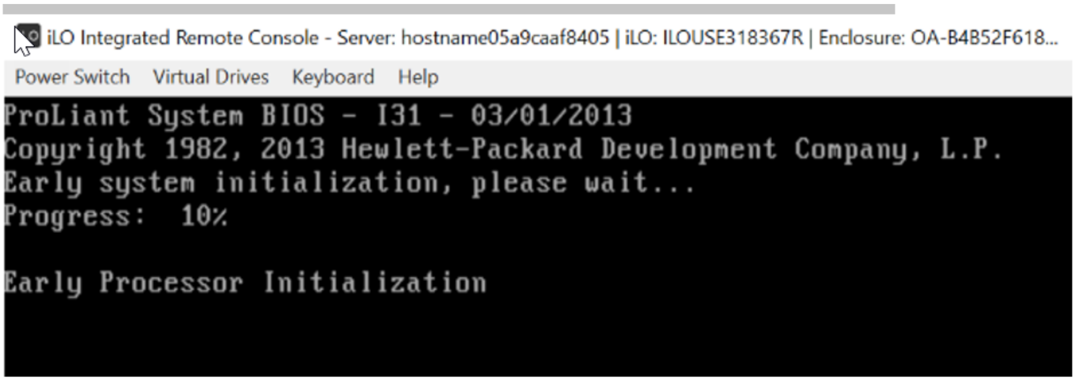

iLO Integrated Remote Console - Server: hostnameb6ccae857233 | iLO: ILOUSE318367N | Enclosure: OA-B4B52F618...
Power Switch
Virtual Drives
Keyboard
Help
□ Folder
□ Image File Removable Media
□ URL Removable Media
☑ Image File CD-ROM/DVD
□ URL CD-ROM/DVD

2. Reboot host, log in to Blade Server ILo GUI browser page and launch remote console.

   To reboot host:
   Click **Power Switch** and select **Reset** from the dropdown menu.


iLO Integrated Remote Console - Server: hostnameb6ccae857233 | iLO: ILOUSE318367N | Enclosure: OA-B4B52F618...
Power Switch
Virtual Drives
Keyboard
Help
Momentary Press
Press and Hold
Cold Boot
Reset

   The remote console window displays that the host is rebooting.



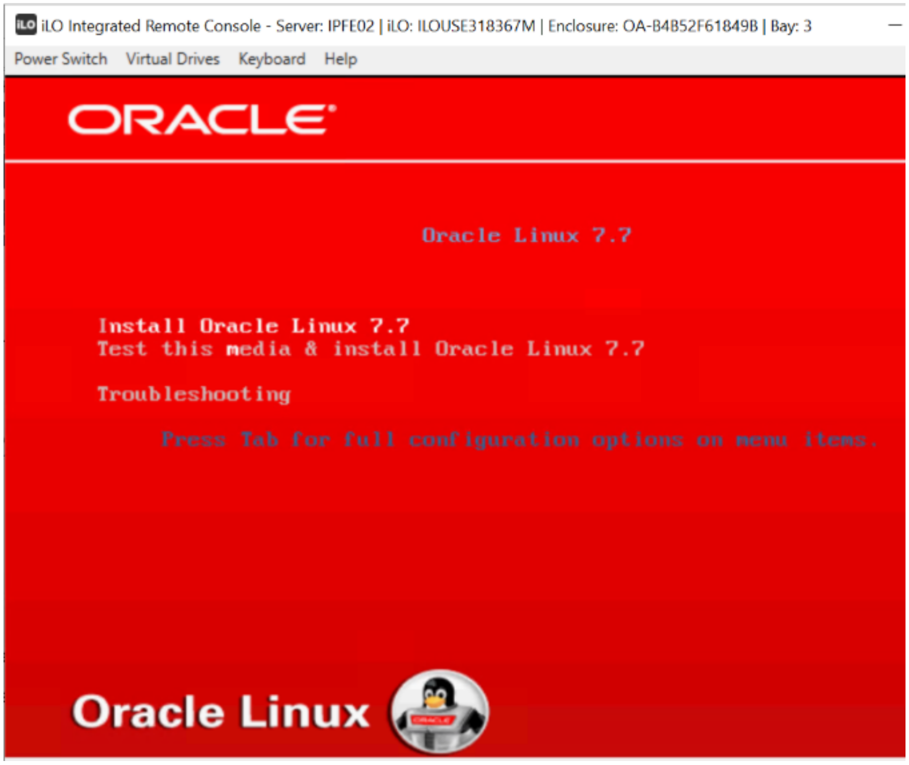
iLO Integrated Remote Console - Server: hostname05a9caaf8405 | iLO: ILOUSE318367R | Enclosure: OA-B4B52F618...

```
ProLiant System BIOS - I31 - 03/01/2013
Copyright 1982, 2013 Hewlett-Packard Development Company, L.P.
Early system initialization, please wait...
Progress:  10%

Early Processor Initialization
```

Wait for a couple of minutes for reboot to complete.

3. Initiate Oracle Linux Platform installation.

   Once reboot completes, the host boots with Oracle Linux installation ISO and the GUI screen prompts for the installation options.



iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F61849B | Bay: 3

```
Oracle Linux 7.7

Install Oracle Linux 7.7
Test this media & install Oracle Linux 7.7

Troubleshooting

      Press Tab for full configuration options on menu items.
```

   Select **Install Oracle Linux 7.x** to continue.

4. Choose Oracle Linux OS language.

   a. When prompted, select **English** as Oracle Linux OS language.

   b. Press **Continue** to go to next step.

5. Set up time zone.

   The next page INSTALLATION SUMMARY displays the required information to start installation.
   Navigate to **Localization**, and then **DATE & TIME**.

- Pick a time zone by selecting a region and city from the drop-down lists, or by clicking a location on the map.
- Choose a country and city that are in the same time zone as your system.

You need to specify a time zone even if you intend to use the Network Time Protocol (NTP) to set the time on the system. Before you can enable NTP, ensure that the system is connected to a network by selecting the **Network & Hostname** option on the INSTALLATION SUMMARY screen.

To enable NTP:

- Switch **ON** the Network Time.
- Click **Settings** button to display a dialog where you can configure the NTP servers used by the system.

To set the date and time manually:

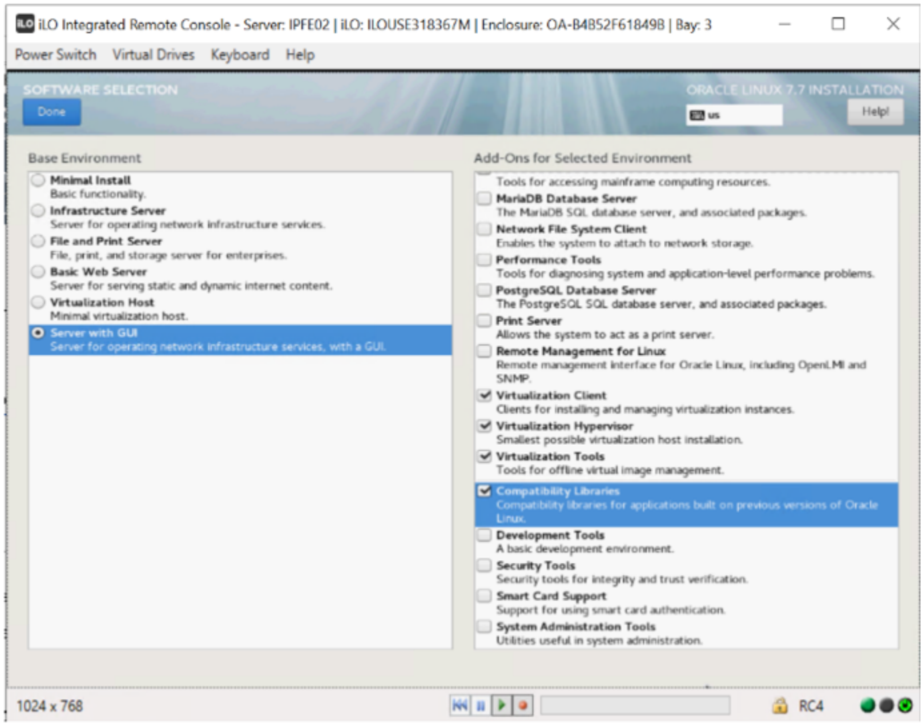
- Switch **OFF** the Network Time
- Adjust the date and time at the bottom of the screen if needed.

Click **Done** to save your configuration and return to the INSTALLATION SUMMARY screen.

6. Setup installation base environment.

   Click **SOFTWARE SELECTION** options in the SOFTWARE area. Select **Server with GUI** from the Base Environment area, and ensure that the following add-ons are selected:

   - Virtualization Client
   - Virtualization Hypervisor
   - Virtualization Tools
   - Compatibility Libraries



iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F61849B | Bay: 3

Base Environment

- ○ **Minimal Install** Basic functionality.
- ○ **Infrastructure Server** Server for operating network infrastructure services.
- ○ **File and Print Server** File, print, and storage server for enterprises.
- ○ **Basic Web Server** Server for serving static and dynamic internet content.
- ○ **Virtualization Host** Minimal virtualization host.
- ● **Server with GUI** Server for operating network infrastructure services, with a GUI.

Add-Ons for Selected Environment

- Tools for accessing mainframe computing resources.
- ☐ **MariaDB Database Server** The MariaDB SQL database server, and associated packages.
- ☐ **Network File System Client** Enables the system to attach to network storage.
- ☐ **Performance Tools** Tools for diagnosing system and application-level performance problems.
- ☐ **PostgreSQL Database Server** The PostgreSQL SQL database server, and associated packages.
- ☐ **Print Server** Allows the system to act as a print server.
- ☐ **Remote Management for Linux** Remote management interface for Oracle Linux, including OpenLMI and SNMP.
- ☑ **Virtualization Client** Clients for installing and managing virtualization instances.
- ☑ **Virtualization Hypervisor** Smallest possible virtualization host installation.
- ☑ **Virtualization Tools** Tools for offline virtual image management.
- ☑ **Compatibility Libraries** Compatibility libraries for applications built on previous versions of Oracle Linux.
- ☐ **Development Tools** A basic development environment.
- ☐ **Security Tools** Security tools for integrity and trust verification.
- ☐ **Smart Card Support** Support for using smart card authentication.
- ☐ **System Administration Tools** Utilities useful in system administration.

Click **Done** to save the changes and go back to the main configuration page.

7. Set up installation destination.

   Click **INSTALLATION DESTINATION** in the SYSTEM area.

   - Select 'sda' (or 'sdb') to use
   - Check **Automatically configure partitioning**
   - Click **Done** to continue

8. Review all the information and click **Begin Installation**.

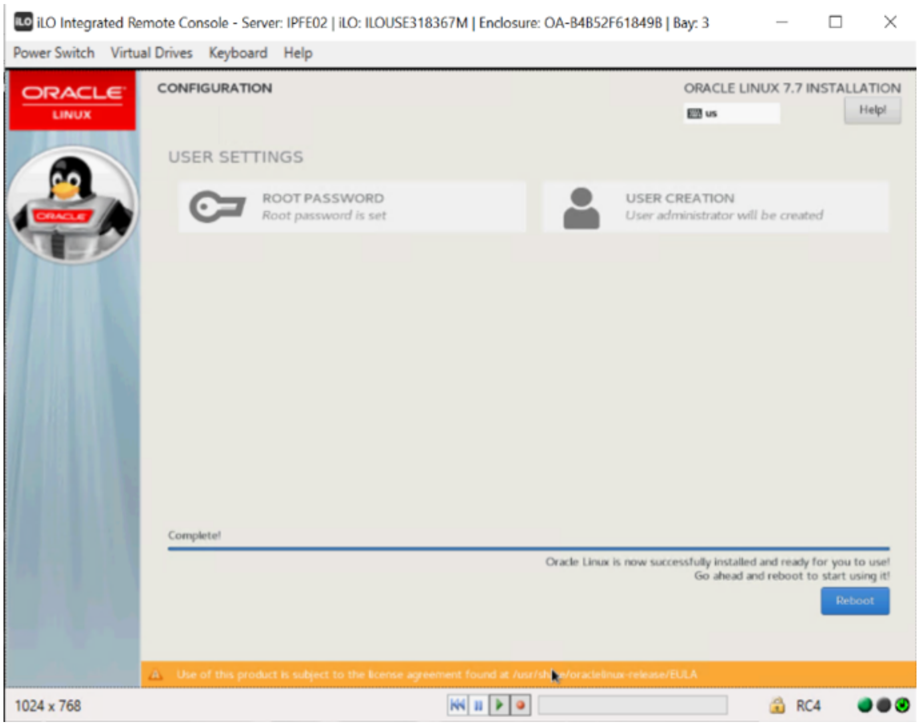
   > **Note**
   >
   > Network configuration is not mandatory at this point and can be performed after Oracle Linux OS is installed.

9. Create login credentials.

   At the same time Oracle Linux installation software lays down files into Gen 10 local hard disk, you may configure root credential or any other login credentials as per the requirement.

10. Reboot host after installation completed.

    Wait for the installation to complete, until the following screen appears.



iLO Integrated Remote Console - Server: IPFE02 | iLO: ILOUSE318367M | Enclosure: OA-B4B52F61849B | Bay: 3

CONFIGURATION

ORACLE LINUX 7.7 INSTALLATION

USER SETTINGS

ROOT PASSWORD
Root password is set

USER CREATION
User administrator will be created

Complete!

Oracle Linux is now successfully installed and ready for you to use!
Go ahead and reboot to start using it!

Use of this product is subject to the license agreement found at /usr/share/oraclelinux-release/EULA

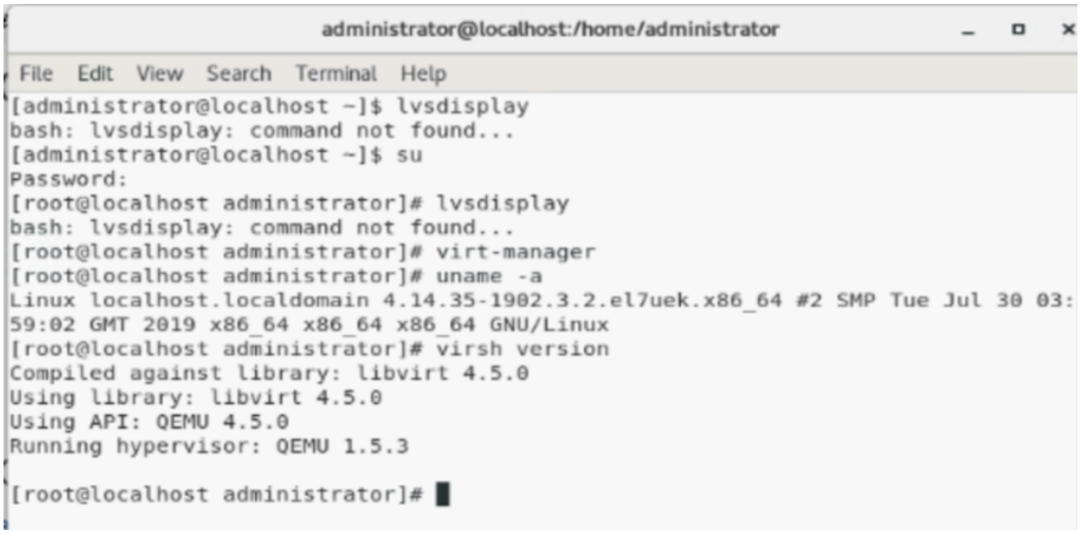
    Click **Reboot** button to reboot.

11. Read and Accept license agreement.

    Check **I accept the license agreement** and click **Finish Configuration** to continue. Skip when prompted for ULN settings.

12. Verify kernel version and KVM version.

Open SSH console window and check following:

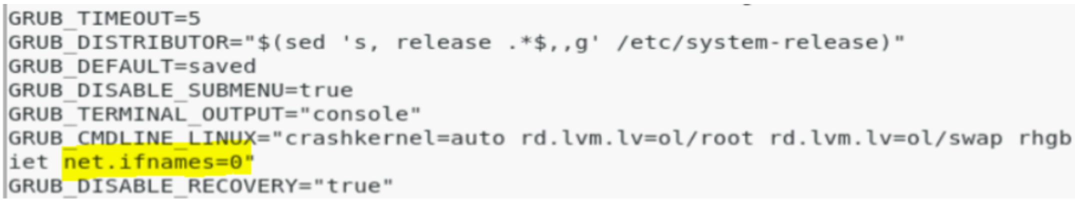

administrator@localhost:/home/administrator
File Edit View Search Terminal Help

```
[administrator@localhost ~]$ lvsdisplay
bash: lvsdisplay: command not found...
[administrator@localhost ~]$ su
Password:
[root@localhost administrator]# lvsdisplay
bash: lvsdisplay: command not found...
[root@localhost administrator]# virt-manager
[root@localhost administrator]# uname -a
Linux localhost.localdomain 4.14.35-1902.3.2.el7uek.x86_64 #2 SMP Tue Jul 30 03:
59:02 GMT 2019 x86_64 x86_64 x86_64 GNU/Linux
[root@localhost administrator]# virsh version
Compiled against library: libvirt 4.5.0
Using library: libvirt 4.5.0
Using API: QEMU 4.5.0
Running hypervisor: QEMU 1.5.3

[root@localhost administrator]# █
```

13. Change network interface name pattern to `ethx`.

    Edit `/etc/default/grub` to append 'net.ifnames=0' with option **GRUB_CMDLINE_LINUX**:

    ```
    [root@localhost ~]# cat /etc/default/grub
    ```

    ```
    GRUB_TIMEOUT=5
    GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
    GRUB_DEFAULT=saved
    GRUB_DISABLE_SUBMENU=true
    GRUB_TERMINAL_OUTPUT="console"
    GRUB_CMDLINE_LINUX="crashkernel=auto rd.lvm.lv=ol/root rd.lvm.lv=ol/swap rhgb
    iet net.ifnames=0"
    GRUB_DISABLE_RECOVERY="true"
    ```

    Recreate the grub2 config file by running:

    ```
    grub2-mkconfig -o /boot/grub2/grub.cfg
    ```

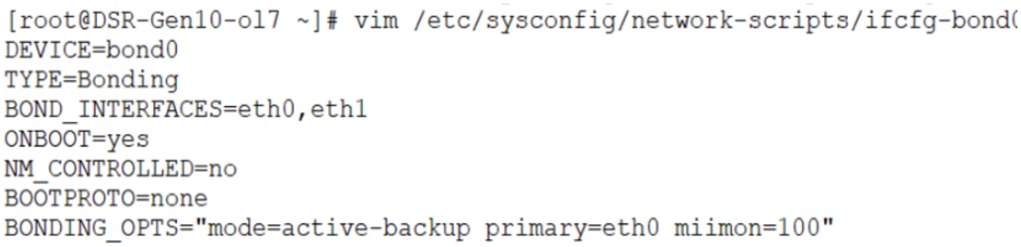
    Restart host and verify that the network interfaces have **ethx** name pattern, by running:

    ```
    shutdown –r
    ```

14. Create bond0 device.

    a. Create device bond0 configuration file:

       ```
       vim /etc/sysconfig/network-scripts/ifcfg-bond0
       ```

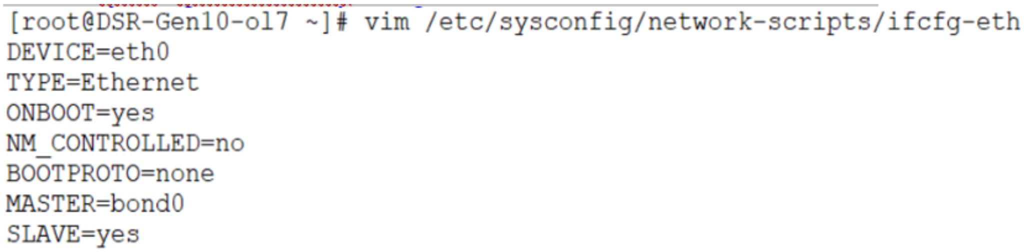


```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-bond
DEVICE=bond0
TYPE=Bonding
BOND_INTERFACES=eth0,eth1
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BONDING_OPTS="mode=active-backup primary=eth0 miimon=100"
```

Save the file and exit.

b. Create device eth0 configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-eth0
```

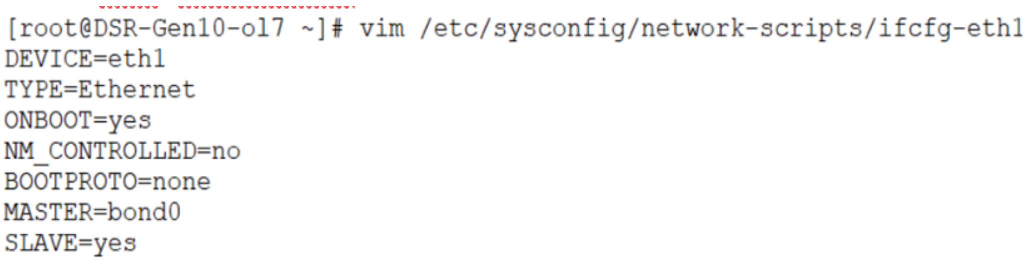


```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
```

Save the file and exit.

c. Create device eth1 configuration file.

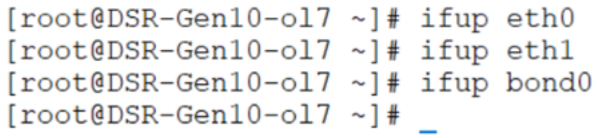
```
vim /etc/sysconfig/network-scripts/ifcfg-eth1
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth1
DEVICE=eth1
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
```

Save the file and exit.

d. Bring up devices into services.

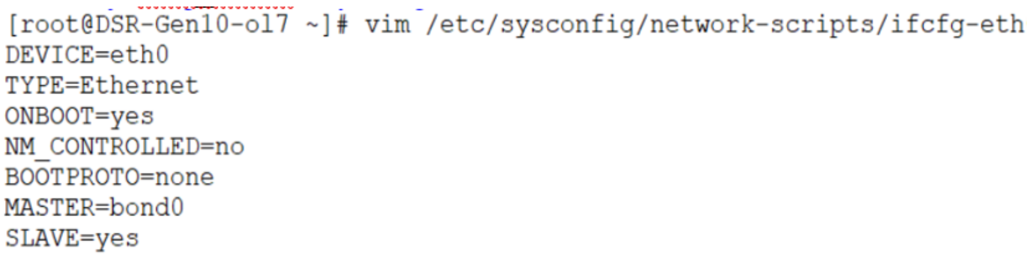


```
[root@DSR-Gen10-ol7 ~]# ifup eth0
[root@DSR-Gen10-ol7 ~]# ifup eth1
[root@DSR-Gen10-ol7 ~]# ifup bond0
[root@DSR-Gen10-ol7 ~]# _
```

15. Create IMI bridge.

a. Create `bond0.<imi_vlan>` configuration file.

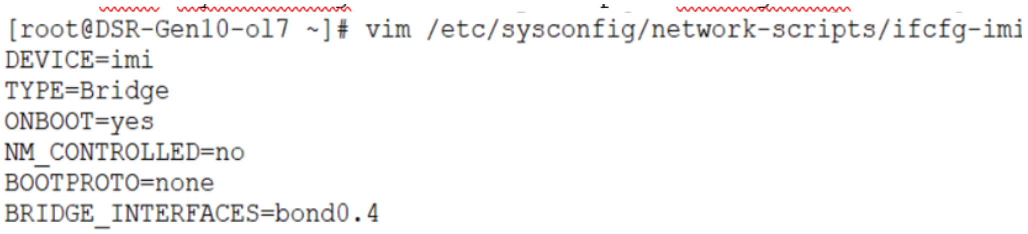
```
vim /etc/sysconfig/network-scripts/ifcfg-bond0.<imi_vlan>
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-eth
DEVICE=eth0
TYPE=Ethernet
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
MASTER=bond0
SLAVE=yes
```

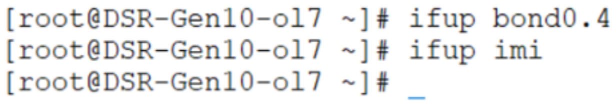
b. Create imi device configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-imi
```



```
[root@DSR-Gen10-ol7 ~]# vim /etc/sysconfig/network-scripts/ifcfg-imi
DEVICE=imi
TYPE=Bridge
ONBOOT=yes
NM_CONTROLLED=no
BOOTPROTO=none
BRIDGE_INTERFACES=bond0.4
```

c. Bring up devices into services.



```
[root@DSR-Gen10-ol7 ~]# ifup bond0.4
[root@DSR-Gen10-ol7 ~]# ifup imi
[root@DSR-Gen10-ol7 ~]# _
```

16. Create XMI bridge.

a. Create `bond0.<xmi_vlan>` configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-bond0.<xmi_vlan>
```

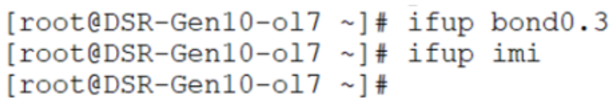
b. Create xmi device configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-xmi
```

c. Set default route for xmi network.

```
vim /etc/sysconfig/network-scripts/route-xmi default via <xmi_gateway>
table main
```

d. Bring up the devices into service.



```
[root@DSR-Gen10-ol7 ~]# ifup bond0.3
[root@DSR-Gen10-ol7 ~]# ifup imi
[root@DSR-Gen10-ol7 ~]#
```

17. Create bond1 device.

a. Create device bond1 configuration file:

```
vim /etc/sysconfig/network-scripts/ifcfg-bond1
```

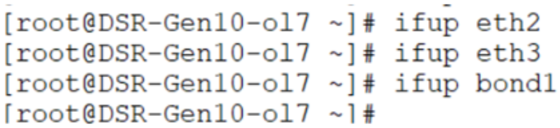
b. Create device eth2 configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-eth2
```

c. Create device eth3 configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-eth3
```

d. Bring up devices into services.



```
[root@DSR-Gen10-ol7 ~]# ifup eth2
[root@DSR-Gen10-ol7 ~]# ifup eth3
[root@DSR-Gen10-ol7 ~]# ifup bond1
[root@DSR-Gen10-ol7 ~]#
```

18. Create xsi1/xsi2 bridge.

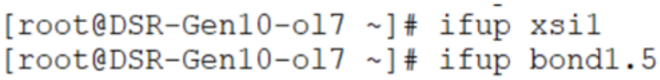
a. Create device `bond1.<xsi1_vlan>` configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-bond1.<xsi1_vlan>
```

b. Create device xsi1 configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-xsi1
```

c. Bring up devices into services.



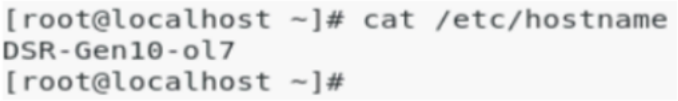
```
[root@DSR-Gen10-ol7 ~]# ifup xsi1
[root@DSR-Gen10-ol7 ~]# ifup bond1.5
```

Note

Perform similar step to create network devices for xsi2.

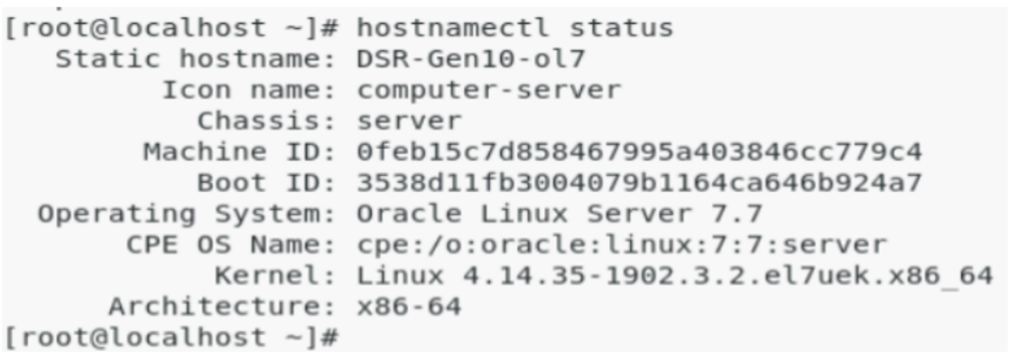
19. Set host name.

a. Rename host by modifying `/etc/hostname` file.



```
[root@localhost ~]# cat /etc/hostname
DSR-Gen10-ol7
[root@localhost ~]#
```

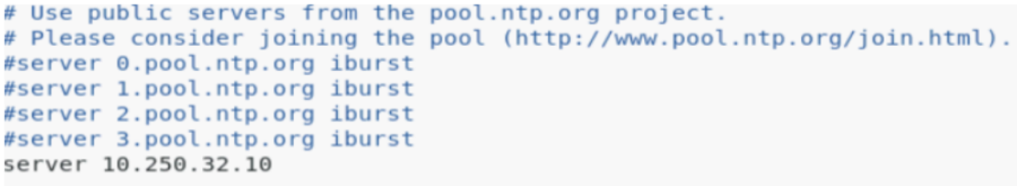
b. Review host name change with following command.



```
[root@localhost ~]# hostnamectl status
   Static hostname: DSR-Gen10-ol7
         Icon name: computer-server
           Chassis: server
        Machine ID: 0feb15c7d858467995a403846cc779c4
           Boot ID: 3538d11fb3004079b1164ca646b924a7
  Operating System: Oracle Linux Server 7.7
       CPE OS Name: cpe:/o:oracle:linux:7:7:server
            Kernel: Linux 4.14.35-1902.3.2.el7uek.x86_64
      Architecture: x86-64
[root@localhost ~]#
```

20. Set NTP service.

    a. Modify `/etc/chrony.conf`, comment out all server * entries and append your NTP server IP to the list with prepending 'server ' text:

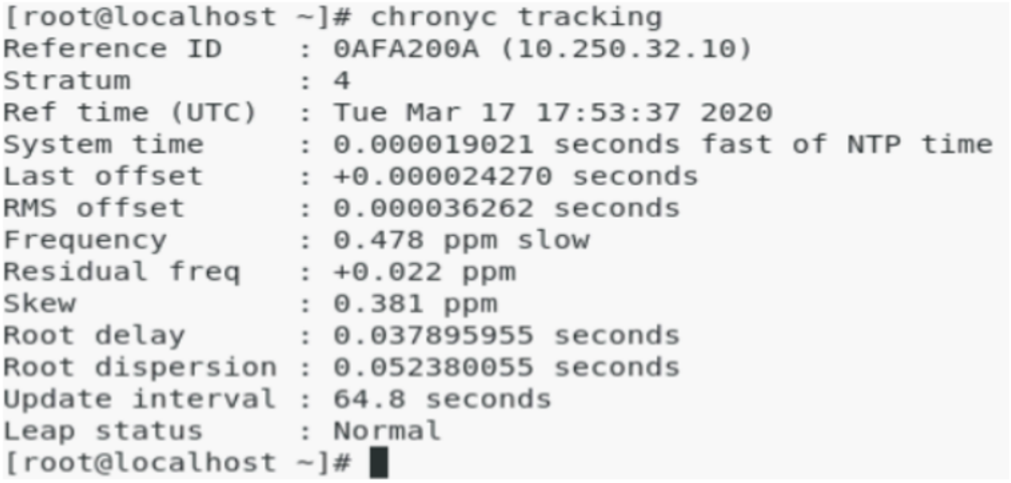


```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
#server 0.pool.ntp.org iburst
#server 1.pool.ntp.org iburst
#server 2.pool.ntp.org iburst
#server 3.pool.ntp.org iburst
server 10.250.32.10
```

    b. Force ntp to sync with newly added server:

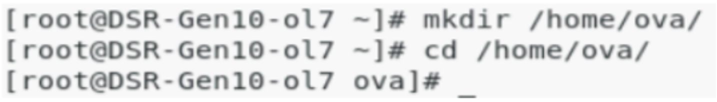
    - `$ ntpdate 10.250.32.10`
    - `$ timedatectl`
    - `$ chronyc tracking`

    c. Verify time synced.



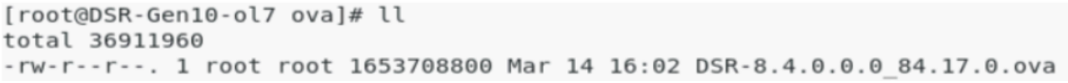
```
[root@localhost ~]# chronyc tracking
Reference ID    : 0AFA200A (10.250.32.10)
Stratum         : 4
Ref time (UTC)  : Tue Mar 17 17:53:37 2020
System time     : 0.000019021 seconds fast of NTP time
Last offset     : +0.000024270 seconds
RMS offset      : 0.000036262 seconds
Frequency       : 0.478 ppm slow
Residual freq   : +0.022 ppm
Skew            : 0.381 ppm
Root delay      : 0.037895955 seconds
Root dispersion : 0.052380055 seconds
Update interval : 64.8 seconds
Leap status     : Normal
[root@localhost ~]# █
```

21. Create `/home/ova` directory.



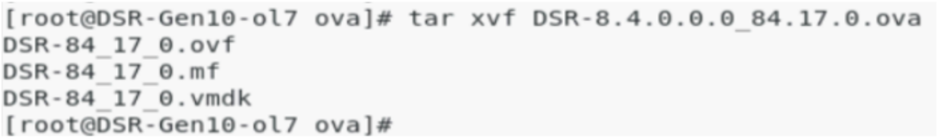
```
[root@DSR-Gen10-ol7 ~]# mkdir /home/ova/
[root@DSR-Gen10-ol7 ~]# cd /home/ova/
[root@DSR-Gen10-ol7 ova]# _
```

22. Transfer OVA file dir using sftp tool.



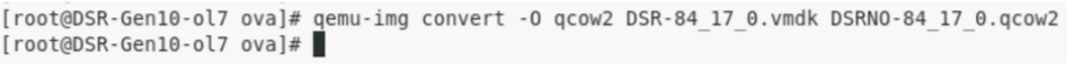
```
[root@DSR-Gen10-ol7 ova]# ll
total 36911960
-rw-r--r--. 1 root root 1653708800 Mar 14 16:02 DSR-8.4.0.0.0_84.17.0.ova
```

23. Untar the ova file.



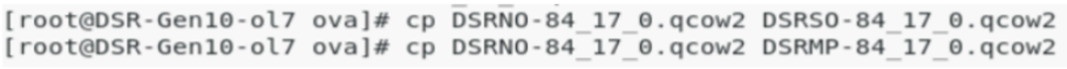
```
[root@DSR-Gen10-ol7 ova]# tar xvf DSR-8.4.0.0.0_84.17.0.ova
DSR-84_17_0.ovf
DSR-84_17_0.mf
DSR-84_17_0.vmdk
[root@DSR-Gen10-ol7 ova]#
```

24. Convert the vmdk file to qcow2 file.



```
[root@DSR-Gen10-ol7 ova]# qemu-img convert -O qcow2 DSR-84_17_0.vmdk DSRNO-84_17_0.qcow2
[root@DSR-Gen10-ol7 ova]# █
```

25. Copy the qcow2 files for SO and MP.



```
[root@DSR-Gen10-ol7 ova]# cp DSRNO-84_17_0.qcow2 DSRSO-84_17_0.qcow2
[root@DSR-Gen10-ol7 ova]# cp DSRNO-84_17_0.qcow2 DSRMP-84_17_0.qcow2
```

26. Configure storage for corresponding qcow2 files as per VMs.
    a. To set the storage for each VM, then run:

       ```
       qemu-img resize <NO_qcow2_filename>.qcow2 <storage_in_gigabytes>G
       ```

    b. Run the command for a VM if storage required is >60G. No need to run this command if the storage required is 60G.
       For example: If resource profile is 2K Sh and VM is NOAMP, whereas the storage required is 70G, then run:

       ```
       qemu-img resize DSRNO-84_17_0.qcow2 70G
       ```

       For multiqueue setting refer to Multiqueue on IPFE (KVM). For Ring buffer, refer Ring Buffer and txqueuelen Configuration (KVM) OL8.9.
27. Set the txqueue length for the ether-net adapter to a high value on the host machine.

Add below script to the above created file `/sbin/ifup-local`

```
[root@DSR-Gen10-ol7 ova]# vim /sbin/ifup-local


ifconfig eth0 txqueuelen 120000
ifconfig eth1 txqueuelen 120000
ifconfig eth2 txqueuelen 120000
ifconfig eth3 txqueuelen 120000
```

28. Verify txqueue length for the ether-net adapter to a high value on the host machine that is added on all interfaces.

    ```
    [root@DSR-Gen10-ol7 ova]# ifconfig <ethernet adapter>
    ```

    Verify same for eth1, eth2, and eth3

29. Restart all ethernet adapters eth0, eth1, eth2, and eth3, one at a time.

    ```
    [root@DSR-Gen10-ol7 ova]# ifdown <ethernet adapter>
    [root@DSR-Gen10-ol7 ova]# ifup <ethernet adapter>
    ```

30. Reboot the host machine.

    ```
    [root@DSR-Gen10-ol7 ova]# reboot
    ```

31. Verify below points on host machinering buffer sizes are set to max on all the ether-net devices txqueue length for all the ether-net adapter to a high value.

    Verify that the following configurations on host machine persist as per the configuration done above:

    - If you have performed Multiqueue configuration on IPFE using Multiqueue on IPFE (KVM), verify the configuration as mentioned the appendix.
    - Ring buffer size setting to max on all the ether-net devices using Step 26.
    - The txqueue length for all the ether-net adapter to a high value using Step 17.

32. Create OCDSR VMs. Repeat this step for each VM.

    To create OCDSR VMs such as NO, SO, MP, IPFE and so on, see Create and Install DSR VMs through KVM GUI. Repeat this procedure for each VM.

33. Add the network device.

    Login to each VM created and add the network devices:

    NO:

    - netAdm add –device=eth0
    - netAdm add –device=eth1

    SO:

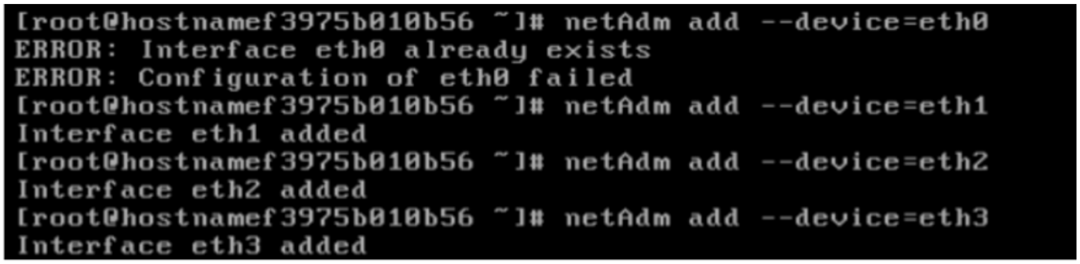
    - netAdm add –device=eth0
    - netAdm add –device=eth1

    MP:

    - netAdm add –device=eth0

- netAdm add –device=eth1
- netAdm add –device=eth2
- netAdm add –device=eth3

For example:



```
[root@hostnamef3975b010b56 ~]# netAdm add --device=eth0
ERROR: Interface eth0 already exists
ERROR: Configuration of eth0 failed
[root@hostnamef3975b010b56 ~]# netAdm add --device=eth1
Interface eth1 added
[root@hostnamef3975b010b56 ~]# netAdm add --device=eth2
Interface eth2 added
[root@hostnamef3975b010b56 ~]# netAdm add --device=eth3
Interface eth3 added
```

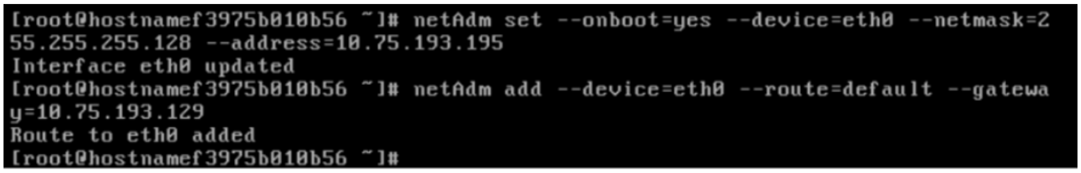
> **Note**
>
> - eth0 is XMI
> - eth1 is IMI
> - eth2 is XSI1
> - eth3 is XSI2 (create eth3 if XSI2 is required)

34. Configure XMI network address.

    Set XMI network address for each DSR VM:

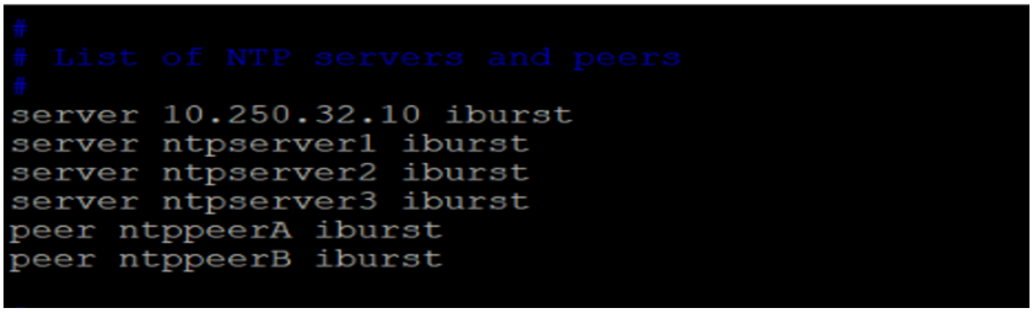
```
netAdm set --device=eth0 --onboot=yes --netmask=<XMI_netmask> --
address=<XMI_network_address>


netAdm add --device=eth0 --route=default --gateway=<XMI_gateway>
```

For example:



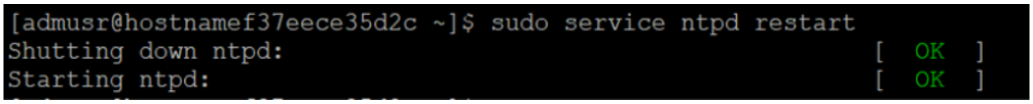
```
[root@hostnamef3975b010b56 ~]# netAdm set --onboot=yes --device=eth0 --netmask=2
55.255.255.128 --address=10.75.193.195
Interface eth0 updated
[root@hostnamef3975b010b56 ~]# netAdm add --device=eth0 --route=default --gatewa
y=10.75.193.129
Route to eth0 added
[root@hostnamef3975b010b56 ~]#
```

35. Configure NTP service.
    a. Configure NTP service for each VM. Run this step on VM.
    b. Open the `/etc/ntp.conf` file and add the NTP servers used in your environment. You can add multiple NTP servers, similar to the examples shown below:



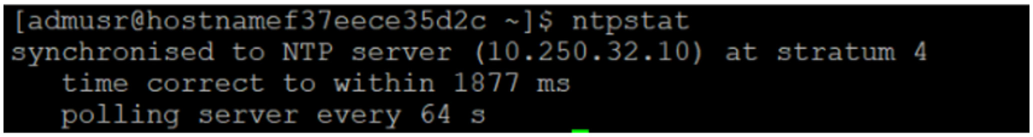
```
#
# List of NTP servers and peers
#
server 10.250.32.10 iburst
server ntpserver1 iburst
server ntpserver2 iburst
server ntpserver3 iburst
peer ntppeerA iburst
peer ntppeerB iburst
```

c. Run the service ntpd start command to start the NTP service and implement the configuration changes.



```
[admusr@hostnamef37eece35d2c ~]$ sudo service ntpd restart
Shutting down ntpd:                                        [  OK  ]
Starting ntpd:                                             [  OK  ]
```

d. Verify ntp status.



```
[admusr@hostnamef37eece35d2c ~]$ ntpstat
synchronised to NTP server (10.250.32.10) at stratum 4
   time correct to within 1877 ms
   polling server every 64 s
```

3.5.2 Create and Install DSR VMs through KVM GUI

This procedure installs DSR VMs NO, SO, and MP using KVM GUI.

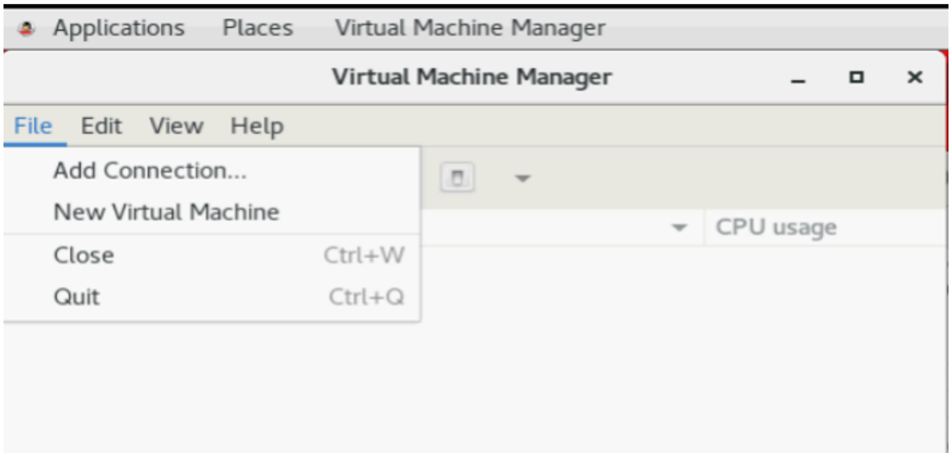
> **Note**
>
> This installation procedure is only applicable for each VM: NO, SO, MP and so on.

Prerequisites:
Installing DSR on OL8 and KVM procedure must be completed.

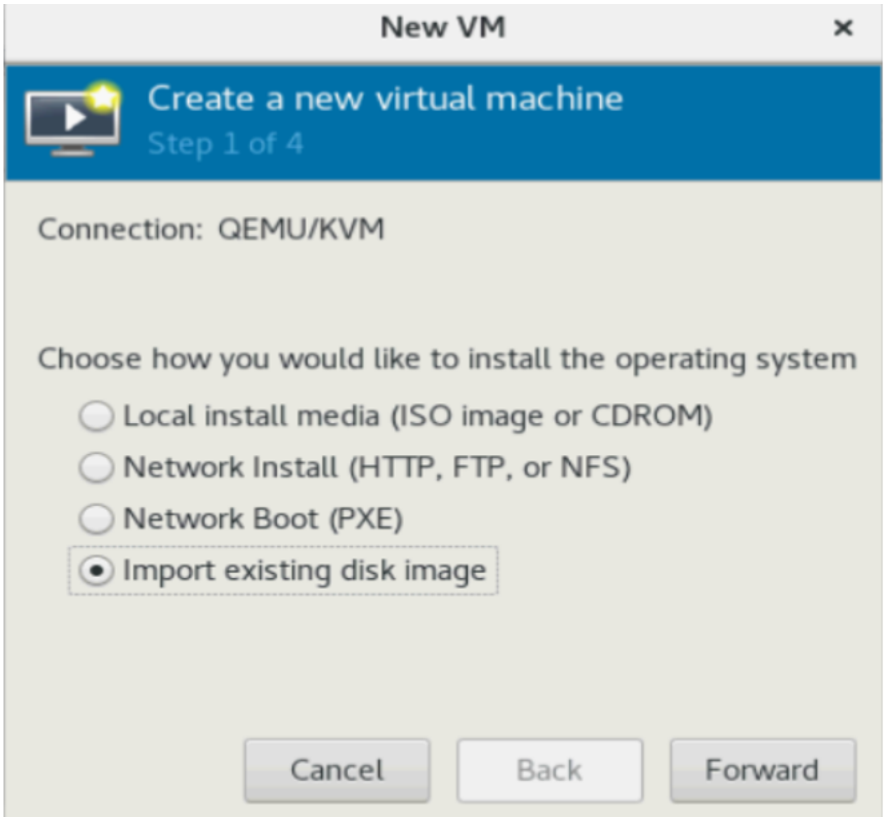
1. Log in to the host machine which has Oracle Linux installed and open the Virtual Machine Manager through CLI, by running:

   ```
   virt-manager
   ```

   > **Note**
   >
   > Ensure X11 forwarding is enabled before running virt-manager command on CLI.



2. Create a new Virtual Machine using the Virtual Manager GUI.
   a. Click **File**, and then **New Virtual Machine**.
   b. Select **Import existing disk image**.



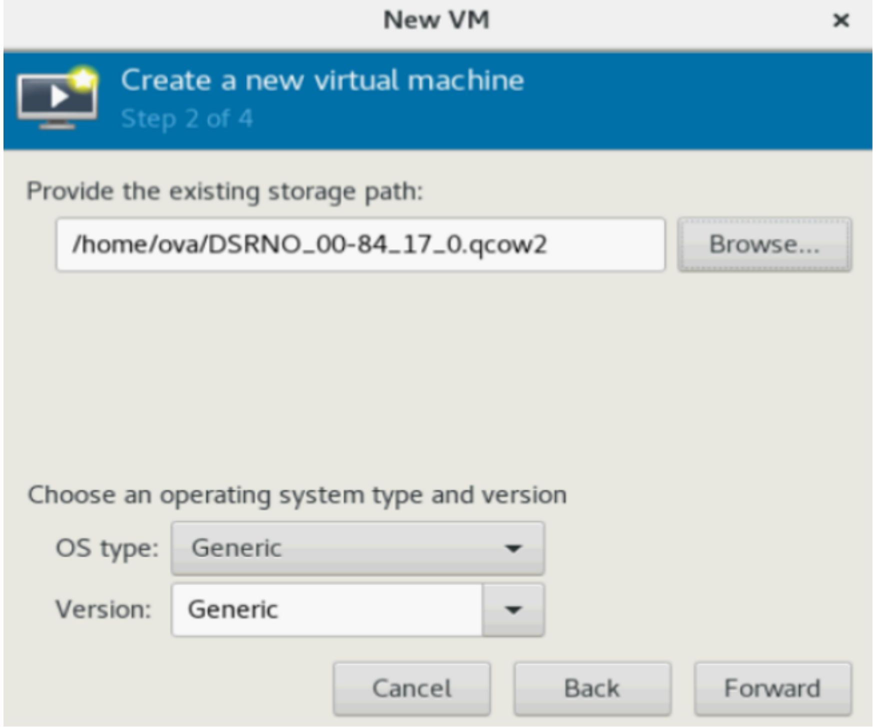
Connection: QEMU/KVM

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

3. Select the qcow2 image by browsing the location `/home/ova` and click **Forward**.

> **Note**
>
> Refer to Installing DSR on OL8 and KVM



New VM

Create a new virtual machine
Step 2 of 4

Provide the existing storage path:

/home/ova/DSRNO_00-84_17_0.qcow2

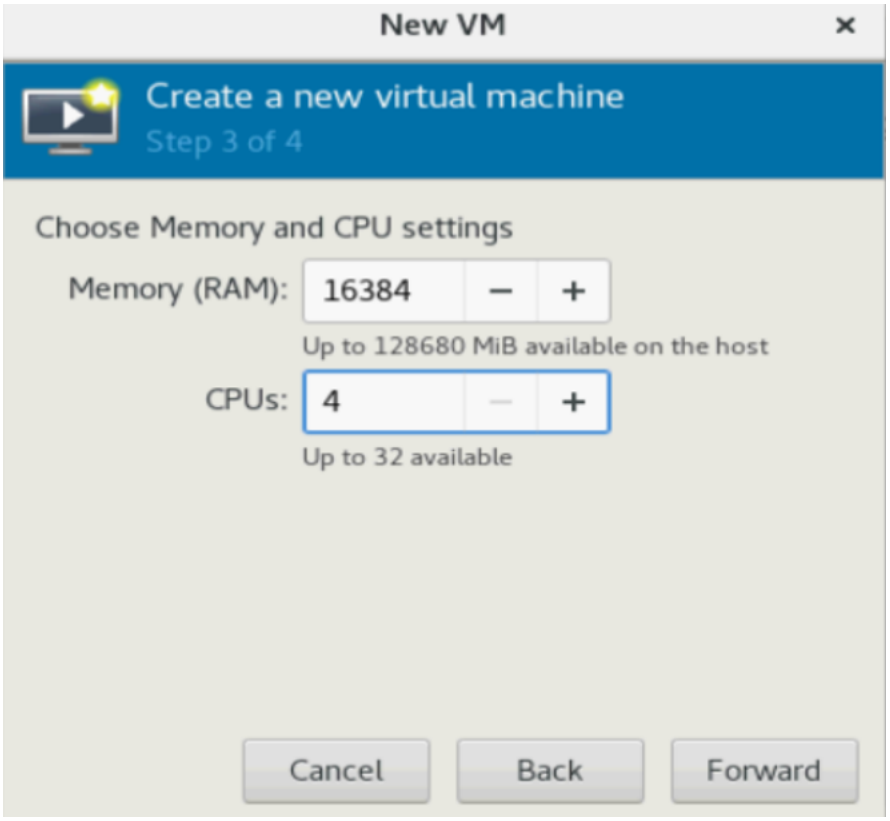
Choose an operating system type and version

OS type: Generic

Version: Generic

4. Select RAM and vCPUs for VM.

   For each VM, select the RAM and vCPUs as per the required resource profile. Then, click **Forward**.



New VM

Create a new virtual machine
Step 3 of 4

Choose Memory and CPU settings

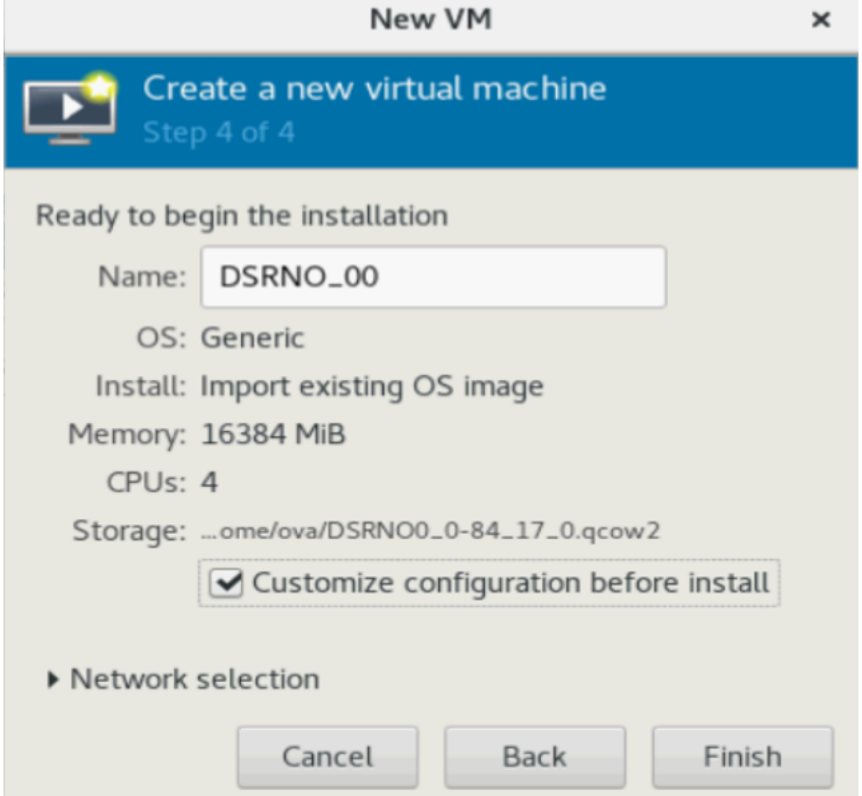
Memory (RAM): 16384

Up to 128680 MiB available on the host

CPUs: 4

Up to 32 available

5. Verify and customize VM.
   a. Update the VM name and select **Customize configuration before install**.
   b. Under **Network selection**, select **XMI bridge** and click **Finish**.



Ready to begin the installation

Name: DSRNO_00

OS: Generic

Install: Import existing OS image

Memory: 16384 MiB

CPUs: 4

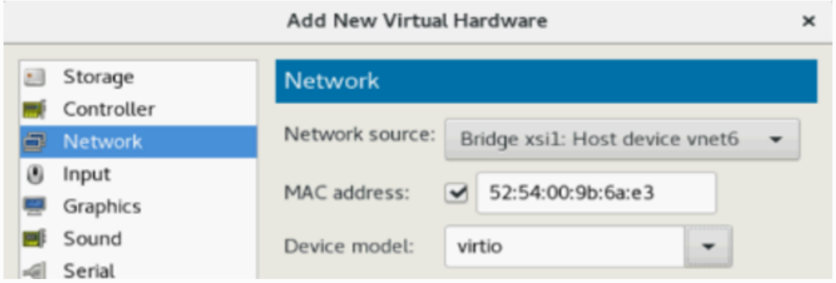
Storage: ...ome/ova/DSRNO0_0-84_17_0.qcow2

☑ Customize configuration before install

6. Modify the Device model to virtio for XMI bridge.
7. Customize the network configuration.
   a. On the next screen, click **Add Hardware**
   b. Select as following:
      - Under Network source, choose the **IMI Bridge**.
      - For NO and SO, choose **IMI bridge only**.
      - For MP, add **XSI1**, along with **IMI** by repeating this step.
   c. Click **Finish**.

Note

Only for MP, we need to add XSI1 & XSI2 bridge as well.
For XSI1 bridge:

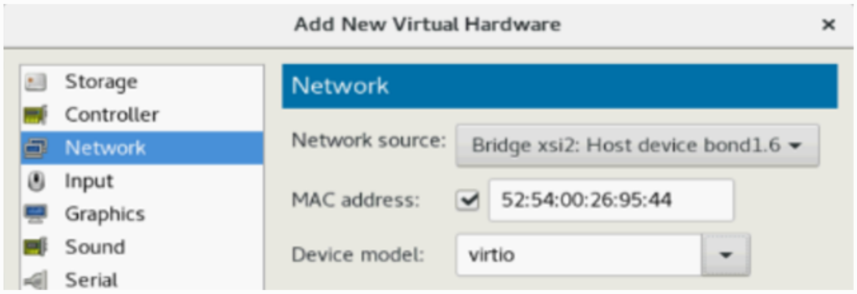


Network source: Bridge xsi1: Host device vnet6

MAC address: ☑ 52:54:00:9b:6a:e3

Device model: virtio

For XSI2 bridge:



Network source: Bridge xsi2: Host device bond1.6

MAC address: ☑ 52:54:00:26:95:44

Device model: virtio

Note

- For DSR Topology it is recommended to add all interfaces on each VM, even when the VM does not require that interface or does not use a VLAN.
- It is just to use a standard when the topology is created from NOAM GUI.

Table 3-4 DSR VMs

DSR VMs	
XMI	eth0
IMI	eth1
XSI1	eth2
XSI2	eth3

Add all interfaces as needed. After adding the other networks, you will see the NICs appear.

Note

- After adding all bridges, verify and begin the VM installation.
- To disable the TSO GSO features for SBR server, see Disabling TSO GSO features for SBR server.

4

Software Installation Using HEAT Templates (OpenStack)

4.1 Prepare OpenStack Template and Environment Files

This procedure gathers required templates and environment files to provide while deploying NOAM or signaling stacks.

Prerequisites
All the respective infrastructures has to be up and running.

1. Log in to the Oracle Document Repository.
2. Select the respective DSR release folder.

   Example: Release 9.2.0.0.0
3. Download the HEAT Templates zip file under **Cloud Installation and Upgrade** section.
4. Unzip the HEAT templates to a folder.
   1. Create a new folder with any name for storing the HEAT templates under the home directory.
      Example: `/home/heat_templates`
   2. Store the downloaded HEAT templates zip file in the folder.
      Example: `/home/heat_templates/exampleHeat.zip`
   3. Unzip the downloaded heat templates.

      ```
      unzip /home/heat_templates/exampleHeat.zip
      ```
5. Determine the template and environment files.

   Below are possible deployment use cases of DSR. The HEAT templates contain files for all scenarios. Determine the appropriate template and environment files with respect to your requirement.

> ⓘ **Note**
>
> Currently, SS7 MPs are not supported. Refer to Example Parameter File.

Table 4-1 Deployment Use Cases

Deployment Use Case	Template Files	Environment Files

Dynamic IP - With VIP	**NOAM Template**
	`dsrNetworkOam_provider.yaml`
	Signaling Template
	`dsrSignalingNode_provider.yaml`
		dsrResources_provider.yaml

Table 4-1 (Cont.) Deployment Use Cases

Deployment Use Case	Template Files	Environment Files

Dynamic IP - Without VIP	**NOAM Template**
	`dsrNetworkOamNoVip_provider.yaml`
	Signaling Template
	`dsrSignalingNodeNoVip_provider.yaml`
		dsrResourcesNoVip_provider.yaml

Fixed IP - With VIP	**NOAM Template**
	`dsrNetworkOam_fixedIps.yaml`
	Signaling Template
	`dsrSignalingNode_fixedIps.yaml`
		dsrResources_fixedIps.yaml

Fixed IP - Without VIP	**NOAM Template** Yet to be created **Signaling Template** Yet to be created.	Yet to be created

Dynamic IP - With IDIH nodes	**NOAM Template**
	`dsrNetworkOam_provider.yaml`
	Signaling Template
	`eidihResources_provider.yaml`
		eidihResources_provider.yaml

Fixed IP - With IDIH nodes	**NOAM Template**
	`dsrNetworkOam_fixedIps.yaml`
	Signaling Template
	`eidihResources_fixedIps.yaml`
		eidihResources_fixedIps.yaml

4.2 Create OpenStack Parameters Files

4.2.1 Create OpenStack Parameter File for NOAM

This procedure instructs how to manually create input parameters file to be provided while deploying NOAM stacks.

Prerequisites:
All the respective infrastructures has to be up and running.

1. Log in to the OpenStack server though command line.
2. Create the parameter file.
   a. Go to the folder created in Prepare OpenStack Template and Environment Files for storing the templates.
   b. Create an empty NOAM parameter file in this folder following this naming convention to identify the purpose of the file.
      `<DSR Name>_<Site Name>_NetworkOam_Params.yaml`

      Example:

      ```
      dsrCloudInit_Site00_NetworkOam_Params.yaml
      ```

ⓘ **Note**

- Refer to Example Template File for a sample file with values.
- It is important to keep the example file ready since this helps you understand the use of each key value pair described in the next step while creating the parameter file.

ⓘ **Note**

- Refer to Example Template File to create the parameter file in YAML format.
- Follow these guidelines while working with the YAML files.
  - The file must end with .yaml extension.
  - YAML must be case-sensitive and indentation-sensitive.
  - YAML does not support the use of tabs. Instead of tabs, it uses spaces.
  - This file is in YAML format and it contains **key:value** pairs.
  - The first key should be **parameters:** and then the remaining required key/value pairs for the topology.

This table lists all required key:value pairs.

Table 4-2 NOAM key:value pairs

Key Name	Type	Description
numPrimaryNoams	number	The number of NOAMs that receive and load DSR topology information **Note:** In DSR 9.2.0.0.0, use 1 as valid value. This NOAM represents active NOAM.
numNoams	number	The number of NOAMs in the DSR topology other than primary NOAM **Note:** In DSR 9.2.0.0.0, use 1 as valid value. This NOAM represents standby NOAM.
noamImage	string	The VM image for the NOAM **Note:** This image is used for both active and standby NOAMs.
noamFlavor	string	The flavor that defines the VM size for the NOAM ⓘ **Note** This flavor is used for both active and standby NOAMs.
primaryNoamVmNames	comma_delimited_list	List of Primary NOAM VM names **Note:** Number of VMnames must be equal to the numPrimaryNoams value.

Table 4-2 (Cont.) NOAM key:value pairs

Key Name	Type	Description
noamVmNames	comma_delimited_list	List of NOAM VM names other than primary NOAM VMs **Note:** Number of VMnames must be equal to the numNoams value.
noamAZ	string	The availability zone into which NOAM servers should be placed **Note:** In DSR 9.2.0.0.0, all NOAM servers are placed in the same availability zone.
noamSG	string	The server group where NOAMs at this site belong
xmiPublicNetwork	string	External management interface
imiPrivateNetwork	string	Internal management interface
imiPrivateSubnet	string	Name of the IMI network
imiPrivateSubnetCidr	string	The address range for the subnet
ntpServer	string	IP of the NTP server
Note: The below 3 keys are only applicable for fixed IP scenario.		
primaryNoamXmiIps	comma_delimited_list	Previously reserved IP for the primary NOAM to talk to external devices
noamXmiIps	comma_delimited_list	Previously reserved IP for non-primary NOAMs to talk to external devices
noamVip	string	VIP for NOAMs

4.2.2 Create OpenStack Parameter File for Signaling

This procedure manually creates the input parameters file to be provided while deploying signaling stacks.

Prerequisites:
All the respective infrastructures have to be up and running.

1. Log in to the OpenStack CLI.
2. Create the parameter file.
   a. Go to the folder created in Prepare OpenStack Template and Environment Files for storing the templates.
   b. Create an empty signaling parameter file in this folder following this naming convention to identify the purpose of the file.
   `<DSR Name>_<Site Name>_SignalingNode_Params.yaml`

   Example:

   ```
   dsrCloudInit_Site00_SignalingNode_Params.yaml
   ```

> **Note**
>
> - Refer to Example Template File for a sample file with values.
> - It is important to keep the example file ready since this helps you understand the use of each key value pair described in the next step while creating the parameter file.

Note

- Refer to Example Template File to create the parameter file in YAML format.
- Follow these guidelines while working with the YAML files.
  - The file must end with .yaml extension.
  - YAML must be case-sensitive and indentation-sensitive.
  - YAML does not support the use of tabs. Instead of tabs, it uses spaces.
  - This file is in YAML format and it contains **key:value** pairs.
  - The first key should be **parameters:** and then the remaining required key/ value pairs for the topology.

This table lists all required key:value pairs.

Table 4-3 Signaling key:value pairs

Key Name	Type	Description
numSoams	number	The number of SOAMs at this signaling node
soamImage	string	The VM image for an SOAM
soamFlavor	string	The flavor that defines the VM size for an SOAM
soamVmNames	comma_delimited_list	List of SOAM VM names
soamAZ	string	The availability zone into which SOAM servers should be placed **Note:** In DSR 9.2.0.0.0, all SOAM servers are placed in the same availability zone.
soamSG	string	Server group for the SOAM VMs
numDas	number	The number of DAs at this signaling node
daImage	string	The VM image for a DA
daFlavor	string	The flavor that defines the VM size for a DA
daVmNames	comma_delimited_list	List of DA VM names
daAZ	string	The availability zone into which DA servers should be placed **Note:** In DSR 9.2.0.0.0, all DA-MP servers are placed in the same availability zone.
daSG	string	Server group for the DA VMs
daProfileName	string	The MP profile to be applied to all DAs. Possible values are: VM_Relay, VM_Database, VM_6K_Mps, VM_8K_Mps, VM_10K_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
numIpfes	number	The number of IPFEs at this signaling node
ipfeImage	string	The VM image for an IPFE
ipfeFlavor	string	The flavor that defines the VM size for an IPFE
ipfeVmNames	comma_delimited_list	List of IPFE VM names
ipfeAZ	string	The availability zone into which IPFE servers should be placed **Note:** In DSR 9.2.0.0.0, all IPFE servers are placed in the same availability zone.
ipfeSGs	comma_delimited_list	Server group for each IPFE VM

Table 4-3 (Cont.) Signaling key:value pairs

Key Name	Type	Description
numStps	number	The number of STPs at this signaling node
stpImage	string	The VM image for an STP
stpFlavor	string	The flavor that defines the VM size for an STP
stpVmNames	comma_delimited_list	List of STP VM names
stpAZ	string	The availability zone into which STP servers should be placed **Note:** In DSR 9.2.0.0.0, all STP servers are placed in the same availability zone.
stpSG	string	Server group for the STP VMs
xmiPublicNetwork	string	External management interface
imiPrivateNetwork	string	Internal management interface
imiPrivateSubnet	string	Name of the IMI network
imiPrivateSubnetCidr	string	The address range for the subnet
xsiPublicNetwork	string	The address range for the subnet
primaryNoamVmName	string	Name of NOAM VM that the config XML was loaded onto **Note:** Not used in 9.2.0.0.0 In DSR 9.2.0.0.0, user should not provide any value to this key.
noamXmiIps	comma_delimited_list	The XMI IPs for all NOAM servers, excluding VIPs **Note:** Not used in 9.2.0.0.0 In DSR 9.2.0.0.0, user should not provide any value to this key.
ntpServer	string	IP of the NTP server
Note: The below keys are ONLY applicable for fixed IP scenario, with or without IDIH nodes.		
soamXmiIps	comma_delimited_list	Previously reserved IP for non-primary SOAMs to talk to external devices
soamVip	string	VIP for SOAMs
daXmiIps	comma_delimited_list	Previously reserved IP for DA MP to talk to external devices
daXsiIps	comma_delimited_list	Previously reserved IP for DA MP to talk to signaling devices
ipfeXmiIps	comma_delimited_list	Previously reserved IP for IPFE to talk to external devices
ipfeXsiIps	comma_delimited_list	Previously reserved IP for IPFE to talk to signaling devices
stpXmiIps	comma_delimited_list	Previously reserved IP for STP to talk to external devices
stpXsiIps	comma_delimited_list	Previously reserved IP for STP to talk to signaling devices
ipfeXsiPublicIp	string	Reserved single IP address on signaling network to which remote diameter hosts route packets for load balancing over set of message processors
stpSctpPorts	comma_delimited_list	The SCTP ports to be associated with STP **Note:** If there is no STP in topology. then provide empty list, for example, [] **Note:** Open these ports beforehand on which STP connections are going to be created while doing configuration.
These two parameters are applicable for TCP/SCTP to use with the Diameter connection. **Note:** Open these ports beforehand on which Diameter connections are going to be created while doing Diameter configuration.		
diameterTcpPorts	comma_delimited_list	The TCP ports to be associated with. If this parameter is not provided, then default ports are assigned.

Table 4-3 (Cont.) Signaling key:value pairs

Key Name	Type	Description
diameterSctpPorts	comma_delimited_list	The SCTP ports to be associated with. If this parameter is not provided, then default ports are assigned.
The below keys are applicable only for scenarios which include IDIH nodes.		
ServiceImage	string	Image used for OpenStack deploys
kafkaImage	string	Image used for OpenStack deploys
mysqlImage	string	Image used for OpenStack deploys
serviceFlavor	string	Flavor used for OpenStack deploys
kafkaFlavor	string	Flavor used for OpenStack deploys
mysqlFlavor	string	Flavor used for OpenStack deploys
kafkaVmName	string	VmName used for OpenStack deploys
serviceVmName	string	VmName used for OpenStack deploys
mysqlVmName	string	VmName used for OpenStack deploys
xmiNetwork	string	Network used to provide access to GUI, ssh, and for inter-site communication.
imiNetwork	string	Internal network for communication between kafka, service and db servers
xsiNetwork	string	Network used for traffic

4.3 Deploy HEAT Templates

This procedure details how to deploy HEAT templates to create NOAM and Signaling stacks.

Prerequisites:
All the respective infrastructures have to be up and running. The required input files are available.

1. Log in to the OpenStack CLI.
2. Prepare the input files required for the deployment.

   To create NOAM and signaling stacks, provide these input files as parameters while deploying the HEAT templates.
   Template Files

   With respect to the deployment scenario decided in Prepare OpenStack Template and Environment Files the template files for NOAM and signaling stacks have been already determined.

   Environment Files

   With respect to the deployment scenario decided in Prepare OpenStack Template and Environment Files the environment files for NOAM and signaling stacks have been already determined.

   Parameter Files

   The parameter file for NOAM has already been created in Create OpenStack Parameter File for NOAM. The parameter file for signaling has already been created in Create OpenStack Parameter File for Signaling.

3. Run the OpenStack command to create NOAM stack using the three input files. Ensure the template and environment files are selected with respect to NOAM stack as in Prepare OpenStack Template and Environment Files.

   ```
   openstack stack create -e <EnvironmentFileForNOAM.yaml> -e
   <ParameterFileForNOAM.yaml> -t <TemplateFileForNOAM> <NOAMStackName>
   ```

   Example for VIP scenario:

   ```
   $ openstack stack create -e dsrResources_provider.yaml -e
   SinglesiteProvider_Site00_NetworkOam_Params.yaml -t
   dsrNetworkOam_provider.yaml SinglesiteProvider_Site00_NetworkOam
   ```

4. Run the OpenStack command to create signaling stack using the three input files. Make sure the template and environment files are selected with respect to signaling stack as per in Prepare OpenStack Template and Environment Files.

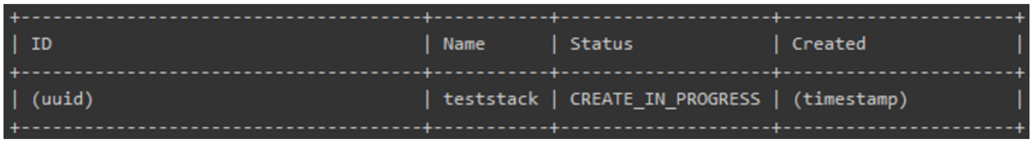
   ```
   openstack stack create -e <EnvironmentFileForSignaling.yaml> -e
   <ParameterFileForSignaling.yaml> -t <TemplateFileForSignaling>
   <SignalingStackName>
   ```

   Example for VIP scenario:

   ```
   $ openstack stack create -e dsrResources_provider.yaml -e
   SinglesiteProvider_Site00_SignalingNode_Params.yaml -t
   dsrSignalingNode_provider.yaml SinglesiteProvider_Site00_Signaling
   ```

5. Verify the stack creation status.
   a. Run this command to see the stack creation status.

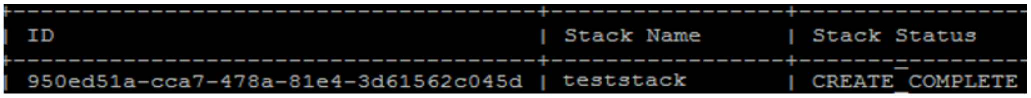
      ```
      $ openstack stack show <stackname>
      ```

      ```
      +--------------------------------------+-----------+--------------------+--------------------+
      | ID                                   | Name      | Status             | Created            |
      +--------------------------------------+-----------+--------------------+--------------------+
      | (uuid)                               | teststack | CREATE_IN_PROGRESS | (timestamp)        |
      +--------------------------------------+-----------+--------------------+--------------------+
      ```

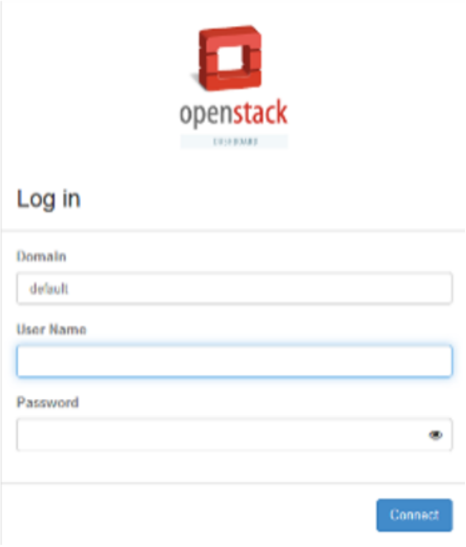
      It takes about two minutes to complete the creation.
   b. Run the command again to verify the status.

      ```
      $ openstack stack show <stackname>
      ```

      ```
      +--------------------------------------+-----------------+-----------------
      | ID                                   | Stack Name      | Stack Status
      +--------------------------------------+-----------------+-----------------
      | 950ed51a-cca7-478a-81e4-3d61562c045d | teststack       | CREATE_COMPLETE
      ```

6. Retrieve required IPs from created stacks.
   a. Log in to the OpenStack GUI with valid credentials.



Log in

Domain

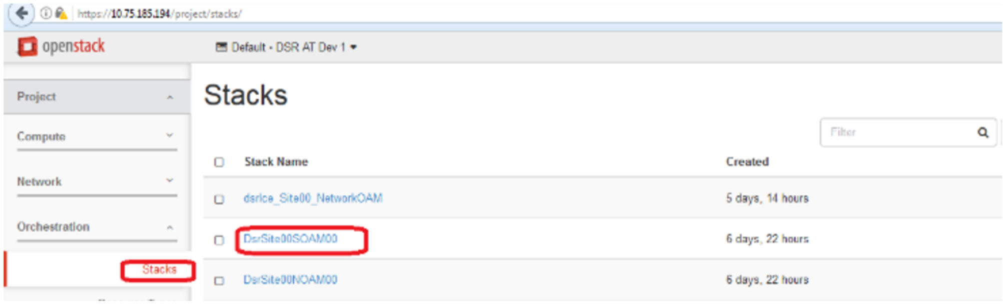
default

User Name

Password

Connect

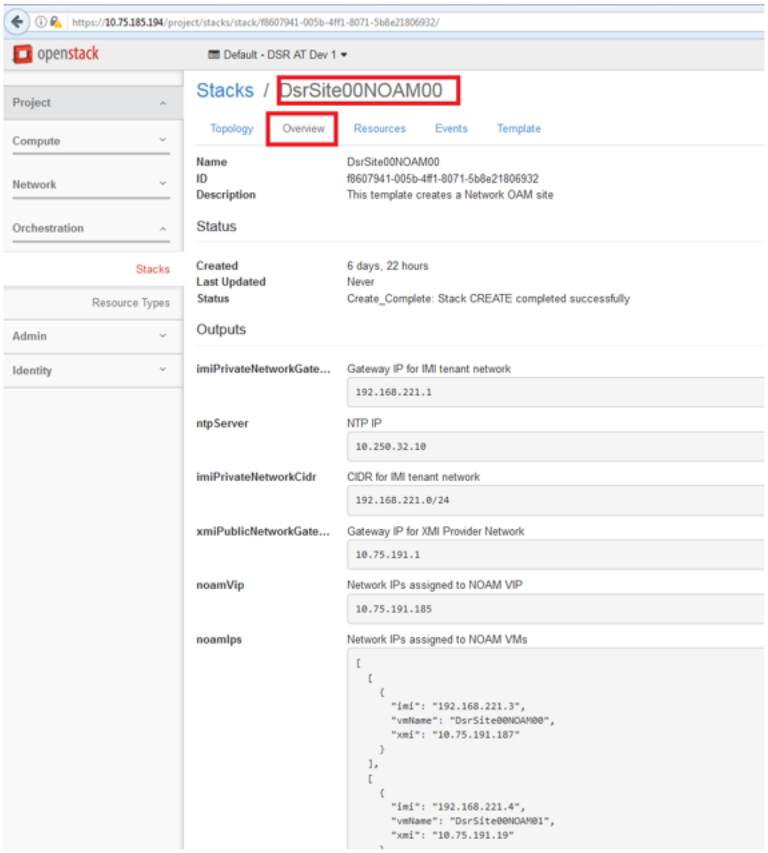
b. Navigate to **Project**, and then **Orchestration** and click **Stacks**.



Stacks

□	Stack Name	Created
□	dsrice_Site00_NetworkOAM	5 days, 14 hours
□	DsrSite00SOAM00	6 days, 22 hours
□	DsrSite00NOAM00	6 days, 22 hours

c. Select the stack you created (<stackname>) and click **Overview** to see the IP details of the stack.



Name	DsrSite00NOAM00
ID	f8607941-005b-4ff1-8071-5b8e21806932
Description	This template creates a Network OAM site

Status

Created	6 days, 22 hours
Last Updated	Never
Status	Create_Complete: Stack CREATE completed successfully

Outputs

imiPrivateNetworkGate... Gateway IP for IMI tenant network

```
192.168.221.1
```

ntpServer NTP IP

```
10.250.32.10
```

imiPrivateNetworkCidr CIDR for IMI tenant network

```
192.168.221.0/24
```

xmiPublicNetworkGate... Gateway IP for XMI Provider Network

```
10.75.191.1
```

noamVip Network IPs assigned to NOAM VIP

```
10.75.191.185
```

noamIps Network IPs assigned to NOAM VMs

```
[
  [
    {
      "imi": "192.168.221.3",
      "vmName": "DsrSite00NOAM00",
      "xmi": "10.75.191.187"
    }
  ],
  [
    {
      "imi": "192.168.221.4",
      "vmName": "DsrSite00NOAM01",
      "xmi": "10.75.191.19"
```

Note

- All NOAM IP information displays in the NOAM stack (<NOAMStackName>).
- All signaling IP information displays in the signaling stack (<SignalingStackName>).

d. Retrieve the IP details for DSR configuration.

5

Application Configuration

Configure the First NOAM NE and Server

This procedure configures the first NOAM VM.

1. Resolve the Hostname to Get Configure the First NOAM NE and Serverthe HTTPD running.
   Change Hostname from the default value using sudo:

   a. Edit `/etc/hosts` file.

      > ⓘ **Note**
      >
      > Remove any occurrence of "**.**" and the "**.<availability zone>**" name, such as "**.novalocal**" from the hostname that might have got appended.

      i. Append the hostname to the IPv4 line as,
         `"127.0.0.1 localhost localhost4 NOAM1"`

      ii. Append the hostname to the IPv6 line as,
         `"::1 localhost localhost6 NOAM1"`

   b. Edit `/etc/syconfig/network`.

      i. Change the "HOSTNAME=XXXX" line to the new hostname.
         `"HOSTNAME=NOAM1"`

      ii. Set the hostname on the command line:
         `$ sudo hostname NOAM1`

   c. Reboot the VM.

      ```
      $ sudo init 6
      ```

2. Establish a NOAM GUI session as the `guiadmin` user on the NOAM server by using the XMI IP address.

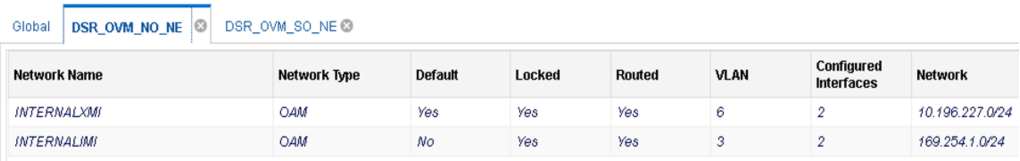
3. In NOAM GUI, create the NOAM network element using the XML file.

   a. Navigate to **Configuration**, and then **Networking**, and then **Networks**.

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

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

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



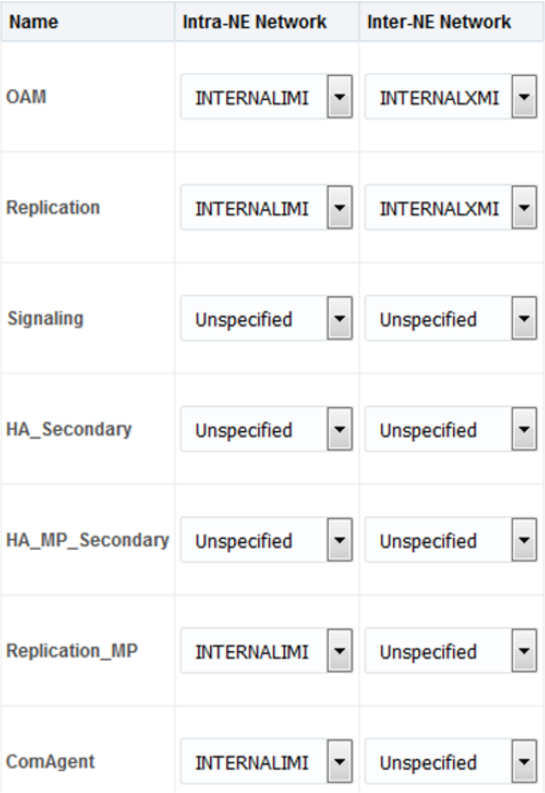
Network Name	Network Type	Default	Locked	Routed	VLAN	Configured Interfaces	Network
INTERNALXMI	OAM	Yes	Yes	Yes	6	2	10.196.227.0/24
INTERNALIMI	OAM	No	Yes	Yes	3	2	169.254.1.0/24

4. In NOAM GUI, map services to networks.
   a. Navigate to **Configuration**, and then **Networking**, and then **Services**.
   b. Click **Edit** and set the services as shown in the table below:

Table 5-1 Network Services

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

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:



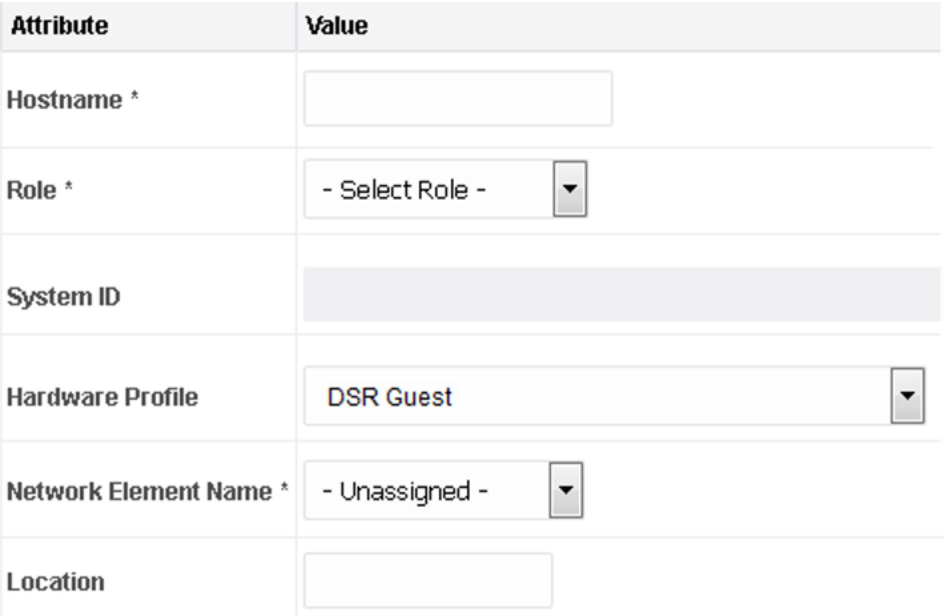
Name	Intra-NE Network	Inter-NE Network
OAM	INTERNALIMI	INTERNALXMI
Replication	INTERNALIMI	INTERNALXMI
Signaling	Unspecified	Unspecified
HA_Secondary	Unspecified	Unspecified
HA_MP_Secondary	Unspecified	Unspecified
Replication_MP	INTERNALIMI	Unspecified
ComAgent	INTERNALIMI	Unspecified

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

5. In NOAM GUI, insert the 1st NOAM VM.

a. Navigate to **Configuration**, and then **Servers**.

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



Attribute	Value
Hostname *	
Role *	- Select Role -
System ID	
Hardware Profile	DSR Guest
Network Element Name *	- Unassigned -
Location	

c. Fill in the fields as follows:
Hostname: <Hostname>

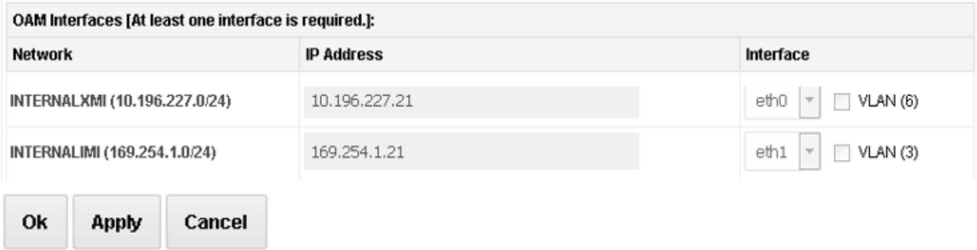
Role: NETWORK OAM&P

System ID: <Site System ID>

Hardware Profile: DSR Guest

Network Element Name: [Select **NE** from drop-down 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)	10.196.227.21	eth0 □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 □ VLAN (3)

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

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

f. Add the following NTP servers:

Table 5-2 NTP Servers

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

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

> **Note**
>
> Properly configure the NTP on the controller node to reference lower stratum NTP servers.

6. In NOAM GUI, export the initial configuration.
   a. Navigate to **Configuration**, and then **Servers**.
   b. 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.
7. In the NOAM Server, copy configuration file to 1st NOAM server.
   a. Log in as an `admusr`, to obtain a terminal window to the 1st NOAM server.
   b. Run the following steps if the setup is IPv6:
      - Run the following command:

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

      - 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 consists a filename such as: `TKLCConfigData.<hostname>`.
      - Following is an example:

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

   c. Run the following step for IPv4 setup:
      - 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 consists a filename such as: `TKLCConfigData..sh`.
      - Following is an example:

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

8. In first NOAM Server, wait for configuration to complete.
   The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.

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

Verify the script completed successfully by checking the following file.

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

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

9. In first NOAM Server, set the time zone (Optional) and reboot the server.
   To change the system time zone, from the command line prompt, run `set_ini_tz.pl`. The following command example uses the America/New_York time zone.

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

   ```
   $ sudo /usr/TKLC/appworks/bin/set_ini_tz.pl
   "America/New_York" >/dev/null 2>&1
   $ date
   $ sudo init 6
   ```

   Wait for server to reboot.

10. In first NOAM Server, verify server health.
    a. Log in to the NOAM1 as the `admusr` user.
    b. Run the following command as `admusr` on the first NOAM server and ensure no errors are returned:

       ```
       $ sudo syscheck
       Running modules in class hardware
               OK
       Running modules in class disk
               OK
       Running modules in class net
               OK
       Running modules in class system
               OK
       Running modules in class proc
               OK
       LOG LOCATION: /var/TKLC/log/syscheck/fail_log
       ```

Configure the NOAM Server Group

This procedure configures the NOAM server group.

1. Log in to NOAM GUI.
   a. 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.

   b. Log in as the `guiadmin` user. If prompted by a security warming, click **Continue to this Website** to proceed.

2. In NOAM GUI, enter NOAM server group data.

   a. Navigate to **Configuration**, and then **Server Groups**.

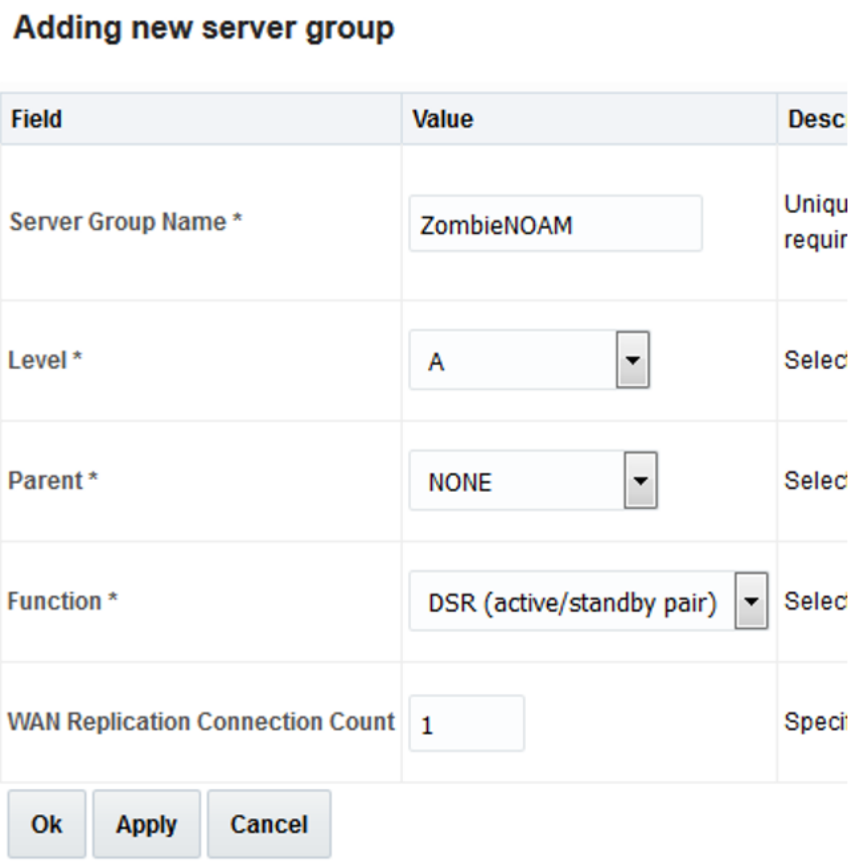
   b. Click **Insert** and fill in the following fields:
   Server Group Name: [Enter Server Group Name]

   Level: A

   Parent: None

   Function: DSR (Active/Standby Pair)

   WAN Replication Connection Count:Use Default Value



Adding new server group

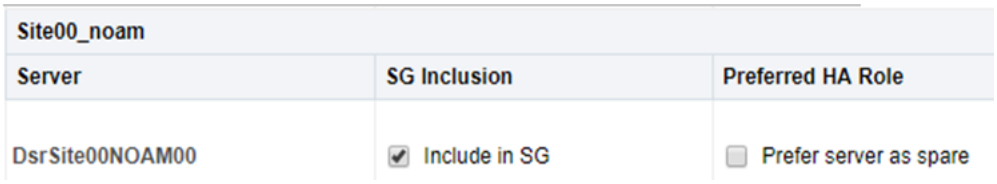
Field	Value	Desc
Server Group Name *	ZombieNOAM	Uniqu requir
Level *	A	Selec
Parent *	NONE	Selec
Function *	DSR (active/standby pair)	Selec
WAN Replication Connection Count	1	Speci

   c. Click **OK** when all fields are filled.

3. In NOAM GUI, edit the NOAM server group.

   a. Navigate to **Configuration**, and then **Server Groups**.

   b. Select the new server group and click **Edit**.
   Select the network element that represents the NOAM.



Site00_noam		
Server	SG Inclusion	Preferred HA Role
DsrSite00NOAM00	☑ Include in SG	□ Prefer server as spare

c. 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.

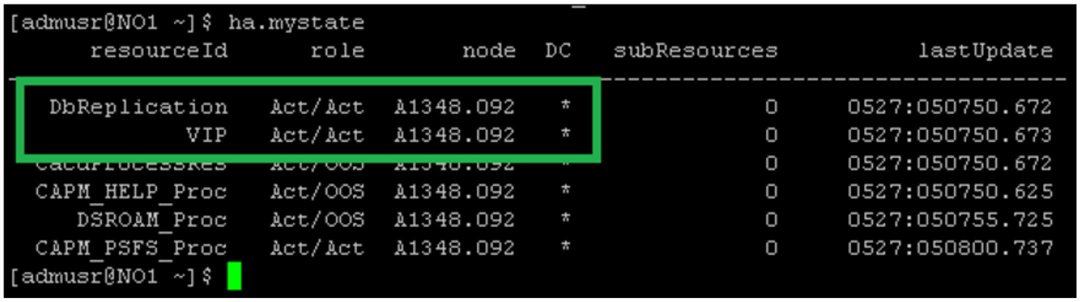
d. Leave the other box unchecked.

e. Click **OK**.

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

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

   Example:



```
[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
    [illegible]       Act/OOS    A1348.092  *              0     0527:050750.672
    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 ~]$
```

5. In NOAM GUI, restart first NOAM VM.

   a. Navigate to **Status & Manage**, and then **Server**.

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

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

6. In NOAM server, set sysmetric thresholds for VMs.

> **Note**
>
> These commands disable the message rate threshold alarms.

From console window of the first NOAM VM, run the `iset` commands as `admusr`:

```
$ sudo iset -feventNumber='-1' SysMetricThreshold  where
"metricId='RoutingMsgRate' and function='DIAM'"
$ sudo iset -feventNumber='-1' SysMetricThreshold  where
"metricId='RxRbarMsgRate' and function='RBAR'"
$ sudo iset -feventNumber='-1' SysMetricThreshold  where
"metricId='RxFabrMsgRate' and function='FABR'"
```

Verify, if the correct value was configured.

Example:

```
$ sudo iqt SysMetricThreshold | grep RxFabrIngressMsgRate


RxFabrMsgRate   FABR  *C RunningAvg   -1   38000     36000      3000
RxFabrMsgRate   FABR  ** RunningAvg   -1   32000     28000      3000
RxFabrMsgRate   FABR  -* RunningAvg   -1   2400      20000      3000
```

Configure the Second NOAM Server

This procedure configures the second NOAM server.

1. Log in to NOAM GUI.
   - a. 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.
   - b. Log in as the `guiadmin` user.
2. In NOAM GUI, insert the second NOAM VM.
   - a. Navigate to **Configuration**, and then **Servers**.
   - b. Click **Insert** to insert the new NOAM server into servers table (the first or server).
   - c. Fill in the fields as follows:
     Hostname: <Hostname>

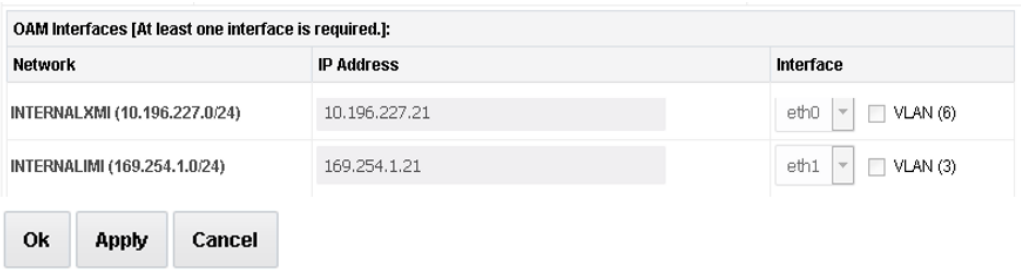
     Role: NETWORK OAM&P

     System ID: <Site System ID>

     Hardware Profile: DSR Guest

     Network Element Name: [Choose **NE** list]

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



OAM Interfaces [At least one interface is required.]:

Network	IP Address	Interface
INTERNALXMI (10.196.227.0/24)	10.196.227.21	eth0 ▾ □ VLAN (6)
INTERNALIMI (169.254.1.0/24)	169.254.1.21	eth1 ▾ □ VLAN (3)

   - d. Fill in the server IP addresses for the XMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unmarked.
   - e. Fill in the server IP addresses for the IMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unmarked.
   - f. Add the following NTP servers:

Table 5-3 NTP Server

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

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

> **Note**
>
> Properly configure the NTP on the controller node to reference lower stratum NTP servers.

3. In NOAM GUI, export the initial configuration.

   a. Navigate to **Configuration**, and then **Servers**.

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

4. In the first NOAM server, copy configuration file to second NOAM server.

   a. Log in as an `admusr` to obtain a terminal session to the 1st NOAM server.

   b. Run the following steps if the setup is IPv6:

      - Log in as an `admusr` user to the NO1 shell and issue the following command:

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

> **Note**
>
> ipaddr is the IP address of NOAM2 assigned to its ethx interface associated with the xmi network.

      - Obtain a terminal session to the 2nd NOAM as an admusr.
      - Run the following commands on NOAM 2 shell:

```
$ sudo rm -f /etc/sysconfig/network-scripts/ifcfg-eth*


sudo cp/var/TKLC/db/filemgmt/TKLCConfigData.sh /var/tmp/
TKLCConfigData.sh
```

   c. Run the following command to setup IPv4:

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

> **Note**
>
> ipaddr is the IP address of NOAM2 assigned to its ethx interface associated with the xmi network.

5. In second NOAM server, wait for configuration to complete.
   1. Obtain a terminal session to the second NOAM as the `admusr` user.
      The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.
   2. If you are on the console, wait to be prompted to reboot the server, but do not reboot the server, it is rebooted later in this procedure.
   3. Verify script completed successfully by checking the following file.

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

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

6. In second NOAM server, reboot the server.
   Obtain a terminal session to the second NOAM as the `admusr` user.

   ```
   $ sudo init 6
   ```

   Wait for server to reboot.
7. In second NOAM server, verify server health.
   1. Log in to the NOAM2 as `admusr` and wait.
   2. Run the following command as super-user on the second NO server and make sure no errors are returned:

      ```
      $ sudo syscheck
      Running modules in class hardware...
              OK
      Running modules in class disk...
              OK
      Running modules in class net...
              OK
      Running modules in class system...
              OK
      Running modules in class proc...
              OK
      LOG LOCATION: /var/TKLC/log/syscheck/fail_log
      ```

Complete the NOAM Server Group Configuration

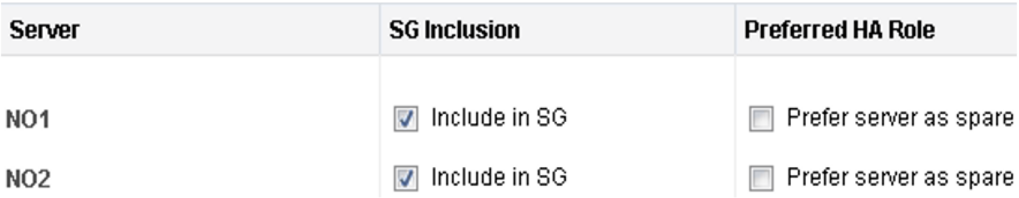
This procedure configures the NOAM Server Group.

1. In NOAM GUI, edit the NOAM Server Group Data.

a. From the GUI session on the first NOAM server, navigate to **Configuration**, and then **Server Groups**.

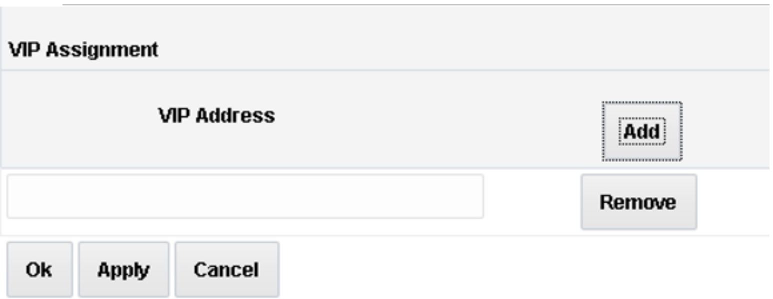
b. Select the NOAM server group and click **Edit**.

c. Add the second NOAM server to the server group by marking the **Include in SG** checkbox for the second NOAM server. Then, click **Apply**.



Server	SG Inclusion	Preferred HA Role
NO1	☑ Include in SG	□ Prefer server as spare
NO2	☑ Include in SG	□ Prefer server as spare

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



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

3. Wait for the alarm ID `10200 Remote Database re-initialization in progress` to be cleared before proceeding to **Alarms & Events**, and then **View Active**.

4. In NOAM GUI, restart the second NOAM VM.

   a. Navigate to **Status & Manage**, and then **Server** and select the second NOAM server.

   b. Click **Restart**.

   c. Click **OK** on the confirmation screen.
   Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the **Appl State** as `Enabled`.

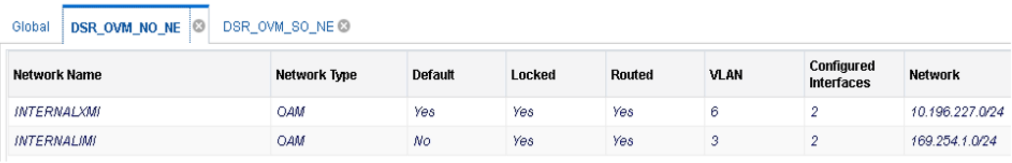
> **Note**
>
> In case you receive alarm, `10073 – Server group max allowed HA Role warning`, perform the following:
>
> i. Log in to the SO GUI and navigate to the **Status & Manage**, and then **HA**.
>
> ii. Click **Edit** and change the **Max Allowed HA role** of the current Standby SOAM to `Active`.

> **Note**
>
> If this deployment contains SDS, SDS can now be installed. Refer to document referenced in *SDS SW Installation and Configuration Guide*.

Configure the DR NOAM NE and Server

This procedure configures the first DR NOAM VM. This is an optional procedure.

1. Establish a GUI session on the primary NOAM server by using the XMI VIP IP address.
2. In primary NOAM VIP GUI, create the DR NOAM network element using the XML file.
   a. Navigate to **Configuration**, and then **Networking**, and then **Networks**.
   b. Click **Browse** and type the pathname to the NOAM network XML file.
   c. Click **Upload File** to upload the XML file.
   See the examples in Sample Network Element and Hardware Profiles and configure the NOAM network element.
   d. Once the data has been uploaded, you should see tabs appear with the name of your network element. Click on the tab, which describes the individual networks that are now configured.



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. In primary NOAM VIP GUI, insert the first DR NOAM VM.
   a. Navigate to **Configuration**, and then **Servers**.
   b. Click **Insert** to insert the new NOAM server into servers table (the first or server).
   c. 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.
   d. Fill in the server IP addresses for the XMI network. Select `ethX` for the interface. Leave the **VLAN** checkbox unchecked.
   e. Fill in the server IP addresses for the IMI network. Select `ethX` for the interface. Leave the **VLAN** checkbox unchecked.
   f. Add the following NTP servers:

Table 5-4 NTP Servers

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

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

> **Note**
>
> Properly configure the NTP on the controller node to reference lower stratum NTP servers.

4. In primary NOAM VIP GUI, export the initial configuration.
   a. Navigate to **Configuration**, and then **Servers**.
   b. 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.
5. In the primary NOAM server, copy configuration file from the first primary NOAM server to the first NOAM at the DRNOAM server.
   a. Log in as an `admusr` to obtain a terminal window to the Primary NOAM server.
   b. Run the following steps if the setup is IPv6:
      - Copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the first NOAM at the DRNOAM server in the `/var/TKLC/db/filemgmt` directory. The configuration file consists a filename like `TKLCConfigData.<hostname>`
      - Following is an example:

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

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

      - Obtain a terminal session to the 1st NOAM at DRNOAM as the admusr.
      - Run the following commands on the 1st Noam at DRNOAM shell.

```
$ sudo rm -f /etc/sysconfig/network-scripts/ifcfg-eth*
```

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

   c. Run the following step to setup IPv4:

- Copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the 1 st NOAM at the DRNOAM server in the `/var/tmp` directory.
- The configuration file consists a filename such as: `TKLCConfigData.<hostname>.sh.`
- Following is an example:

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

6. In first DR NOAM server, wait for configuration to complete.
   The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.

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

   Verify the script completed successfully by checking the following file.

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

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

7. In first DR NOAM server, reboot the server.
   Obtain a terminal window to the 1st DR NOAM server, logging in as the `admusr` user.

   ```
   $ sudo init 6
   ```

   Wait for server to reboot.

8. In first DR NOAM server, verify server health.

   a. Obtain a terminal window to the first DR NOAM server, logging in as the `admusr` user.

   b. Run the following command as `admusr` and ensure that no errors are returned:

      ```
      $ sudo syscheck
      Running modules in class hardware...
              OK
      Running modules in class disk...
              OK
      Running modules in class net...
              OK
      Running modules in class system...
              OK
      Running modules in class proc...
              OK
      LOG LOCATION: /var/TKLC/log/syscheck/fail_log
      ```

Configure the DR NOAM Server Group

This procedure configures the DR NOAM server group. This is an optional procedure.

1. Log in to primary NOAM VIP GUI.
   1. Establish a GUI session on the primary NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type `http://<NO1_XMI_IP_Address>` as the URL.
   2. Log in as the `guiadmin` user. If prompted by a security warming, click **Continue to this Website** to proceed.
2. In primary NOAM VIP GUI, enter DR NOAM server group data.
   1. Using the GUI session on the primary NOAM server, navigate to **Configuration**, and then **Server Groups**.
   2. Click **Insert** and fill in the following fields:
      Server Group Name: [Enter Server Group Name]

      Level: A

      Parent: None

      Function: DSR (Active/Standby Pair)

      WAN Replication Connection Count:Use Default Value
   3. Click **OK** when all fields are filled.
3. In primary NOAM VIP GUI, edit the DR NOAM server group.
   1. Navigate to **Configuration**, and then **Server Groups**.
   2. Select the new server group and click **Edit**.
   3. Select the network element that represents the DR NOAM.
   4. In the portion of the screen that lists the servers for the server group, find the NOAM server being configured. Mark the **Include in SG** checkbox.
   5. Leave other boxes unchecked.
   6. Click **OK**.
4. In primary NOAM VIP GUI, restart first DR NOAM VM.
   1. From the NOAM GUI, navigate to **Status & Manage**, and then **Server**.
   2. Select the first NOAM server. Click **Restart**.
   3. Click **OK** on the confirmation screen and wait for restart to complete.

Configure the Second DR NOAM Server

This procedure configures the second DR NOAM server. This is an optional procedure.

1. Log in to primary NOAM VIP GUI.
   1. If not already done, establish a GUI session on the first NOAM server by using the XMI IP address of the first NOAM server. Open the web browser and type `http://<NOAM1_XMI_IP_Address>` as the URL.
   2. Log in as the `guiadmin` user.
2. In primary NOAM VIP GUI, insert the second DR NOAM VM.
   1. Navigate to **Main Menu**, and then **Configuration**, and then **Servers**.

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

c. 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.

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

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

f. Add the following NTP servers:

Table 5-5 NTP Servers

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

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

> **Note**
>
> Properly configure the NTP on the controller node to reference lower stratum NTP servers.

3. In primary NOAM VIP GUI, export the initial configuration.

   a. Navigate to **Configuration**, and then **Servers**.

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

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

4. In the primary NOAM, copy configuration file to second DR NOAM server.

   a. Login as an `admusr` to obtain a terminal session to the primary NOAM server.

   b. Run the following steps if the setup is IPv6:

      - Copy the configuration file created in the previous step from the `/var/TKLC/db/filemgmt` directory on the 2nd DR-NOAM server in the `/var/TKLC/db/filemgmt` directory.

      - The configuration file consists a filename such as: `TKLCConfigData.<hostname>.sh`.

- Following is an example:

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

- Obtain a terminal session to the 2nd DRNOAM as an admusr.
- Run the following commands on 2nd DRNOAM shell:

  ```
  $ sudo rm -f /etc/sysconfig/network-scripts/ifcfg-eth*


  sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.sh /var/tmp/
  TKLCConfigData.sh
  ```

c. Run the following step to setup IPv4:

- Log in as the `admusr` user to the NOAM1 shell and issue the following command:

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

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

5. In second DR NOAM server, wait for configuration to complete.

a. Obtain a terminal session to the second DR NOAM as the `admusr` user.
The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.

b. If you are on the console, wait to be prompted to restart the server, but do not restrt the server, it is restarted later in this procedure.

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

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

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

6. In second DR NOAM server, restart the server.
Obtain a terminal session to the second DR NOAM as the `admusr` user.

```
$ sudo init 6
```

Wait for server to reboot.

7. In second DR NO server, verify server health.

a. Obtain a terminal session to the second DR NOAM as the `admusr` user.

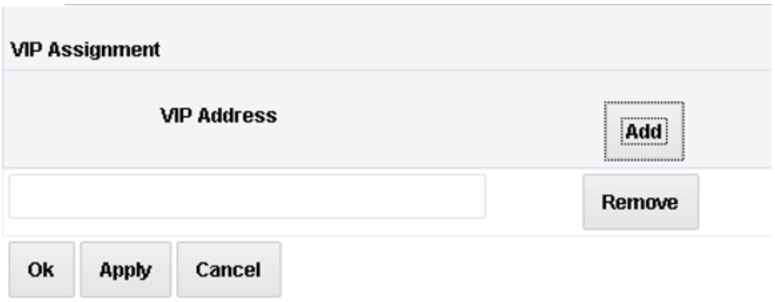
b. Run the following command as super-user and make sure no errors are returned:

```
$ sudo syscheck
Running modules in class hardware...
        OK
Running modules in class disk...
        OK
Running modules in class net...
        OK
Running modules in class system...
        OK
Running modules in class proc...
        OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

Complete Configuring the DR NOAM Server Group

This procedure finishes configuring the DR NOAM Server Group. This is an optional procedure.

1. In primary NOAM VIP GUI, edit the DR NOAM server group data.
   a. From the GUI session on the primary NOAM server, navigate to **Configuration**, and then **Server Groups**.
   b. Select the NOAM server group and click **Edit**.
   c. Add the second NOAM server to the server group by marking the **Include in SG** checkbox for the second NOAM server. Then, click **Apply**.
   d. Click **Add** to add an NOAM VIP. Type the `VIP Address` and click **OK**.



2. Establish a GUI session on the primary NOAM by using the NOAM VIP address. Login as the `guiadmin` user.
3. In primary NOAM VIP GUI, wait for the alarm `ID 10200 Remote Database re-initialization` in progress to be cleared before proceeding to **Alarms & Events**, and then **View Active**.
4. In primary NOAM VIP GUI, restart second DR NOAM VM.
   a. Navigate to **Status & Manage**, and then **Server** and select the second DR NOAM server.
   b. Click **Restart**.
   c. Select **OK** on the confirmation screen.
   Wait approximately 3-5 minutes before proceeding to allow the system to stabilize indicated by having the **Appl State** as `Enabled`.

5. In primary NOAM, modify DSR OAM process.
Establish an SSH session to the primary NOAM, login as the `admusr` user. Run the following commands:
   a. Retrieve the cluster ID of the DR-NOAM:

```
$ sudo iqt -NodeID TopologyMapping where "NodeID='<DR_NOAM_Host_Name>' "
Server_ID     NodeID                 ClusterID
1             Oahu-DSR-DR-NOAM-2     A1055
```

   b. Run the following command to start the DSR OAM process on the DR-NOAM.

```
$ echo "<clusterID>|DSROAM_Proc|Yes" | iload -ha -xun cluster –
fresource –foptional HaClusterResourceCfg
```

Configure the SOAM NE

This procedure configures the SOAM network element.

1. If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the **guiadmin** user.
2. In primary NOAM VIP GUI, create the SOAM network element using an XML file.
Ensure 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 Configure the First NOAM NE and Server, but defines the SOAM network element.

   Refer to Sample Network Element and Hardware Profiles for a sample network element xml file.
   a. Navigate to **Configuration**, and then **Networking**, and then **Networks**.
   b. Click **Browse** and type the path and name of the SOAM network XML file.
   c. Click **Upload** to upload the XML file and configure the SOAM network element.

Configure the SOAM Servers

This procedure configures the SOAM servers.

1. If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the `guiadmin` user.
2. In primary NOAM VIP GUI, insert the first SOAM server.
   a. Navigate to **Configuration**, and then **Server**.
   b. Click **Insert** to insert the new SOAM server into servers table.
   c. 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.
   d. Fill in the server IP addresses for the XMI network. Select **ethX** for the interface. Leave the **VLAN** checkbox unmarked.

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

f. Add the following NTP servers:

Table 5-6 NTP Servers

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

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

> ⓘ **Note**
>
> Properly configure the NTP on the controller node to reference lower stratum NTP servers.

3. In primary NOAM VIP GUI, export the initial configuration.

   a. Navigate to **Configuration**, and then **Server**.

   b. From the GUI screen, select the desired server and click **Export** to generate the initial configuration data for that server.

   c. Go to the **Info** tab to confirm the file has been created.

4. In the primary NOAM, copy configuration file to the first SOAM server.Log in as an `admusr` user to the NOAM1 shell and issue the commands:

   a. Run the following steps if the setup is IPv6:

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

> ⓘ **Note**
>
> ipaddr is the IP address of 1st SOAM assigned to its ethx interface associated with the xmi network.

- Obtain a terminal session to the 1st SOAM as the admusr.
- Run the following commands on 1st SOAM shell:

```
$ sudo rm -f /etc/sysconfig/network-scripts/ifcfg-eth*
```

```
sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.sh /var/tmp/
TKLCConfigData.sh
```

b. Run the following command to setup IPv4:

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

5. In the first SOAM server, wait for configuration to complete.

   a. Obtain a terminal session on the first SOAM as the `admusr` user.
   The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.

   b. 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.

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

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

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

6. In first SOAM server, reboot the server.
   Obtain a terminal session to the first SOAM as the `admusr` user.

   ```
   $ sudo init 6
   ```

   Wait for server to reboot.

7. In first SOAM server, verify server health.

   a. After the system reboots, login again as the `admusr` user.

   b. Run the following command and make sure that no errors are returned:

   ```
   # sudo syscheck
   Running modules in class hardware...
           OK
   Running modules in class disk...
           OK
   Running modules in class net...
           OK
   Running modules in class system...
           OK
   Running modules in class proc...
           OK
   LOG LOCATION: /var/TKLC/log/syscheck/fail_log
   ```

8. Repeat steps 1 through 7 to insert and configure the second SOAM server.

   a. Run the following steps if the setup is IPv6:

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

> **Note**
>
> ipaddr is the IP address of 2nd SOAM assigned to its ethx interface associated with the xmi network.
>
> - Obtain a terminal session to the 2nd SOAM as the admusr.
> - Run the following commands on 2nd SOAM shell.
>
> ```
> $ sudo rm -f /etc/sysconfig/network-scripts/ifcfg-eth*
>
>
> sudo cp /var/TKLC/db/filemgmt/TKLCConfigData.sh /var/tmp/
> TKLCConfigData.sh
> ```

b. Run the following command to setup IPv4:

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

c. Wait approximately 5 minutes for the 2nd SOAM server to restart

> **Note**
>
> For DSR mated sites, repeat this step for additional or spare SOAM server.

.
Enter the network data for the second SOAM server, transfer the `TKLCConfigData` file to the second SOAM server, and reboot the second SOAM server when asked at a terminal window.

d. Wait approximately 5 minutes for the second SOAM server to reboot.

> **Note**
>
> For DSR mated sites, repeat this step for additional/spare SOAM server for mated site.

Configure the SOAM Server Group

This procedure configures the SOAM server group.

1. In primary NOAM VIP GUI, enter SOAM server group data.

   a. From the GUI session on the NOAM VIP address, navigate to **Configuration**, and then **Server Groups**.

   b. Click **Insert** and add the SOAM server group name along with the values for the following fields:
   Name: [Enter Server Group Name]

   Level: B

   Parent: [Select the NOAM Server Group]

Function: DSR (Active/Standby Pair)

WAN Replication Connection Count: Use Default Value

c. Click **OK** when all fields are filled.

> ⓘ **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.

2. In primary NOAM VIP GUI, edit the SOAM server group and add VIP.

   a. Navigate to **Configuration**, and then **Server Groups**.

   b. Select the new SOAM server group and click **Edit**.

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

   d. Click **Apply**.

3. In primary NOAM VIP GUI, add the SOAM VIP.

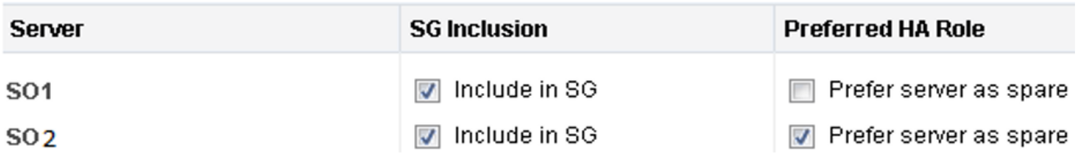
   a. Navigate to **Configuration**, and then **Server Groups**.

   b. Select the new SOAM server group and click **Edit**.

   c. Click **Add** to add a SOAM VIP. Type the `VIP Address` and click **OK**.

4. In primary NOAM VIP GUI, edit the SOAM server group and add preferred spares for site redundancy.
   This is an optional step.

   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.

Server	SG Inclusion	Preferred HA Role
SO1	☑ Include in SG	□ Prefer server as spare
SO2	☑ Include in SG	☑ Prefer server as spare

   For more information about server group secondary site or site redundancy, see the Terminology section.

5. In primary NOAM VIP GUI, edit the SOAM server group and add additional SOAM VIPs.
   This is an optional step.

   a. Click **Add** to add SOAM VIPs.

   b. Type the **VIP Address** and click **OK**.

> ⓘ **Note**
>
> Additional SOAM VIPs only apply to SOAM server groups with preferred spare SOAMs.

6. In primary NOAM VIP GUI, wait for replication.

After replication, the server status should be active. Navigate to **Status & Manage**, and then **HA**.

> **Note**
>
> This may take up to 5 minutes while the servers figure out primary or secondary relationship.

Look for the alarm ID `10200 Remote Database re-initialization in progress` to be cleared before proceeding. Navigate to **Alarms**, and then **View Active**.

7. In primary NOAM VIP GUI, restart first SOAM server.
   1. From the NOAM GUI, navigate to **Status & Manage**, and then **Server** and select the first SOAM server.
   2. Click **Restart**.
   3. Click **OK** on the confirmation screen.
      Wait for restart to complete. Wait for the **Appl State** to change to `Enabled`, and all other columns to `Norm`.

      > **Note**
      >
      > Repeat this step for the second SOAM.

8. In primary NOAM VIP GUI, restart all preferred spare SOAM servers.
   This is an optional step.
   1. If additional preferred spare servers are configured for secondary sites, navigate to **Status & Manage**, and then **Server** and select all the Preferred Spare SOAM servers.
   2. Click **Restart** and then, click **OK** to the confirmation popup.
      Wait for the **Appl State** to change to **Enabled** and all other columns to change to `Norm`.

Activate PCA/DCA

This procedure activates PCA/DCA. This is applicable only for PCA and DCA.

1. Activate PCA feature.
   If you are installing PCA, run the applicable procedures (Added SOAM site activation or complete system activation) of the *DSR PCA Activation Guide* 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.
   > - Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

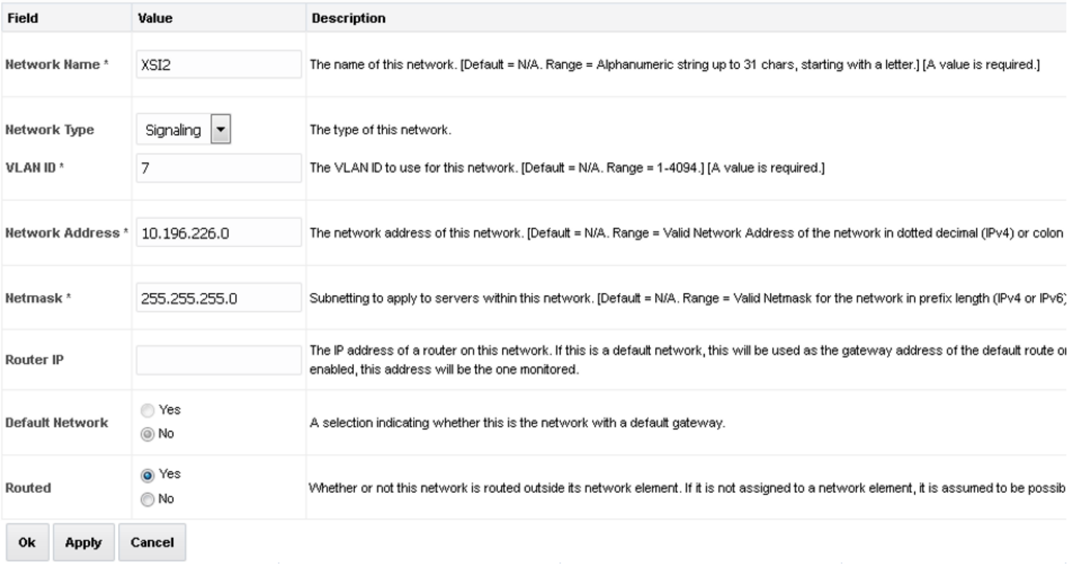
2. Activate DCA feature.
   If you are installing PCA, run *DCA Framework and Application Activation and Deactivation Guide* to activate the DCA framework and feature.

> **Note**
>
> - If not all SOAM sites are ready at this point, then you should repeat activation for each new SOAM site that comes online.
> - Ignore steps to restart DA-MPs and SBRs that have yet to be configured.

Configure the MP Virtual Machines

This procedure configures MP VMs (IPFE, SBR, DA-MP, and vSTP).

1. If needed, establish a GUI session on the NOAM by using the NOAM VIP address. Login as the `guiadmin` user.
2. In primary NOAM VIP GUI, navigate to the signaling network configuration screen.
   a. Navigate to **Configuration**, and then **Networking**, and then **Networks**.
   b. Navigate to the **SO Network Element** tab under which the MPs are to be configured.
   c. Click **Insert** in the lower left corner.
3. In primary NOAM VIP GUI, add signaling networks.
   The following screen displays.



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 o enabled, this address will be the one monitored.
Default Network	○ Yes ● No	A selection indicating whether this is the network with a default gateway.
Routed	● Yes ○ 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 possib

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

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

      i. Select **Signaling** for Network Type.
      ii. Select **No** for Default Network.

iii. Select **Yes** for Routable.

b. If you are finished adding signaling networks, click **OK**. To save this signaling network and repeat this step to enter additional signaling networks, click **Apply** .

4. In primary NOAM VIP GUI, navigate to signaling network configuration screen.

> ⓘ **Note**
>
> Run this step only if you are defining a separate, dedicated network for SBR Replication. This step is applicable only for PCA or DCA.

a. Navigate to **Configuration**, and then **Networking**, and then **Networks**.

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

5. In primary NOAM VIP GUI, define SBR DB replication network.

> ⓘ **Note**
>
> Run this step only if you are defining a separate, dedicated network for SBR replication. This is applicable only for PCA.

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

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

i. Select **No** for Default Network.

ii. Select **Yes** for Routable.

b. If you are finished adding signaling networks, click **OK**. To save this signaling network and repeat this step to enter additional signaling networks, click **Apply** .

6. In primary NOAM VIP GUI, perform additional service to networks mapping.

> ⓘ **Note**
>
> Run this step only if you are defining a separate, dedicated network for SBR replication. This is only applicable to PCA.

a. Navigate to **Configuration**, and then **Networking**, and then **Services**.

b. Click **Edit**.

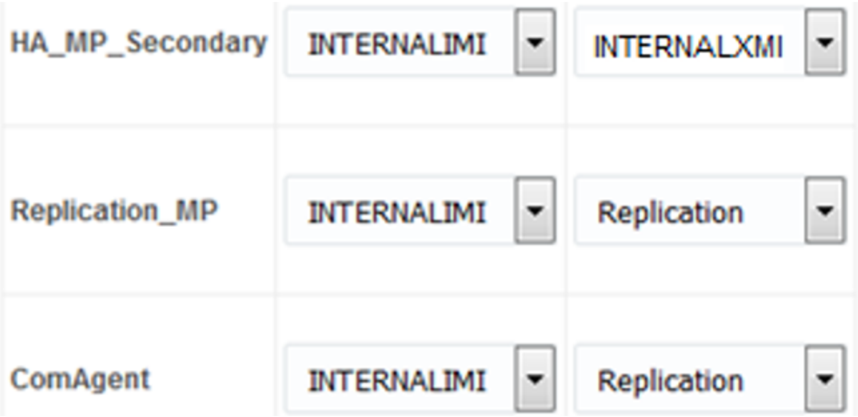
c. Set the services using one of the following scenarios.

- If the dual-path HA configuration is required:
  For HA_MP_Secondary, Oracle recommends the inter-NE network is set as the XMI network and intra-NE network is set as the IMI network. If the primary

interface (Replication_MP) SBR DB Replication Network interface goes down, use the secondary network for sharing HA status to reduce the likelihood of a split brain. This leads to DSR mate isolation from the active SBR and results in traffic loss until SBR DB Replication Network is down.

Table 5-7 Replication Network

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>

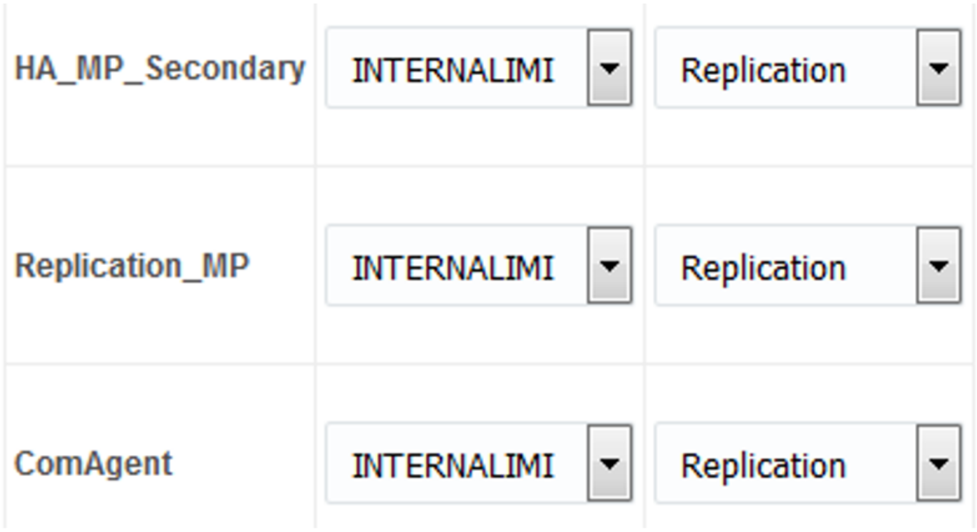


HA_MP_Secondary	INTERNALIMI	INTERNALXMI
Replication_MP	INTERNALIMI	Replication
ComAgent	INTERNALIMI	Replication

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

Table 5-8 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>



HA_MP_Secondary	INTERNALIMI	Replication
Replication_MP	INTERNALIMI	Replication
ComAgent	INTERNALIMI	Replication

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

7. In primary NOAM VIP GUI, insert the MP or IPFE server – Part 1.

   a. Navigate to **Configuration**, and then **Servers**.

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

   c. Fill in the following values:
   Hostname: <Hostname>

   Role: MP

   System ID: <Site System ID>

   Hardware Profile: DSR Guest

   Network Element Name: [Choose **NE** from list]

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

   e. Leave the **VLAN** checkbox unmarked.

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

      i. Leave the **VLAN** checkbox unmarked.

      ii. For the Replication network, type the MP's XSI2 IP address. This is the IP address should be used from the name defined in step 5. This name would be the same name that is referred to as **SBR DB Replication Network** in step 6. Select the correct interface.

   g. For the XSI1 network, type the MP's XSI1 IP address. Select the correct interface.

   > **Note**
   >
   > Leave the **VLAN** checkbox unmarked.

   h. For the XSI2 network, type the MP's XSI2 IP address. Select the correct interface.

> ⓘ **Note**
>
> - Leave the **VLAN** checkbox unmarked.
> - 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.

i. Add the following NTP servers:

Table 5-9 NTP Servers

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

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

> ⓘ **Note**
>
> Properly configure the NTP on the controller node to reference lower stratum NTP servers.

8. In primary NOAM VIP GUI, export the initial configuration.
   a. Navigate to **Configuration**, and then **Networking**, and then **Servers**.
   b. From the GUI screen, select the server that was just configured and click **Export** to generate the initial configuration data for that server.
   c. Go to the Info tab to confirm the file has been created.
9. In MP server, log into the MP.
   Obtain a terminal window connection on the MP or IPFE server.
10. In the primary NOAM VIP GUI, copy configuration file to MP or IPFE server.
    a. From the active NOAM console, login as the `admusr` user.
    b. Run the following steps if the setup is IPv6:

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

       > ⓘ **Note**
       >
       > ipaddr is the IP address of MP/IPFE assigned to its ethx interface associated with the xmi network.

       - Obtain a terminal session to the MP or IPFE as an admusr.

- Run the following commands on MP or IPFE shell:

  ```
  $ sudo rm -f /etc/sysconfig/network-scripts/ifcfg-eth*
  ```

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

c. Run the following command to setup IPv4:

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

   > **Note**
   >
   > ipaddr is the XMI IP address of the MP or IPFE.

11. In MP server, wait for configuration to complete.
    a. Obtain a terminal session on the MP or IPFE as the `admusr` user.
       The automatic configuration daemon looks for the file named `TKLCConfigData.sh` in the `/var/tmp` directory, implements the configuration in the file, and prompts the user to reboot the server.
    b. 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.
    c. Verify script completed successfully by checking the following file.

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

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

12. In MP server, reboot the server.
    Obtain a terminal session on the MP or IPFE as the `admusr` user.

    ```
    $ sudo init 6
    ```

    Wait for server to reboot.

13. In MP server, verify server health.
    a. After the reboot, login as the `admusr` user.
    b. Run the following command as super-user on the server and make sure that no errors are returned:

       ```
       $ sudo syscheck
       Running modules in class hardware...
               OK
       Running modules in class disk...
               OK
       ```

```
Running modules in class net...
        OK
Running modules in class system...
        OK
Running modules in class proc...
        OK
LOG LOCATION: /var/TKLC/log/syscheck/fail_log
```

14. In MP server, delete auto-configured default route on MP and replace it with a Network Route using the XMI Network.

> **Note**
>
> This step is optional and should only be run to configure a default route on your MP that uses a signaling (XSI) network instead of the XMI network. Not running 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.

a. Log into the MP as the `admusr` user. Alternatively, you can log into the VM's console.

b. Determine `<XMI_Gateway_IP>` from your SO site network element information.

c. Gather the following items:
<NO_XMI_Network_Address>

<NO_XMI_Network_Netmask>

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

d. Create network routes to the NO's XMI (OAM) network.

i. Navigate to NOAM VIP GUI **ConfigurationNetworkingRoutes**.

ii. Select the Specific MP.

iii. Click **Insert**.

iv. Enter details.

v. Click **OK**.

e. In MP console if sending SNMP traps from individual servers, create host routes to customer SNMP trap destinations on the XMI network:

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

f. Route to `<MP_XMI_Interface>` added.

g. Repeat for any existing customer NMS stations.

h. Delete the existing default route:

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

Route to `<MP_XMI_Interface>` removed.

i. In MP console, ping active NO XMI IP address to verify connectivity:

```
$ ping <ACTIVE_NO_XMI_IP_Address>
PING 10.240.108.6 (10.240.108.6) 56(84) bytes of data.
64 bytes from 10.240.108.6: icmp_seq=1 ttl=64 time=0.342 ms
64 bytes from 10.240.108.6: icmp_seq=2 ttl=64 time=0.247 ms
```

j. In MP console, ping customer NMS Station(s):

```
$ ping <Customer_NMS_IP>
PING 172.4.116.8 (172.4.118.8) 56(84) bytes of data.
64 bytes from 172.4.116.8: icmp_seq=1 ttl=64 time=0.342 ms
64 bytes from 172.4.116.8: icmp_seq=2 ttl=64 time=0.247 ms
```

k. 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.

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

Configure Places and Assign MP Servers to Places

This procedure adds places in the PCA, and DCA networks. This is applicable only for PCA and DCA.

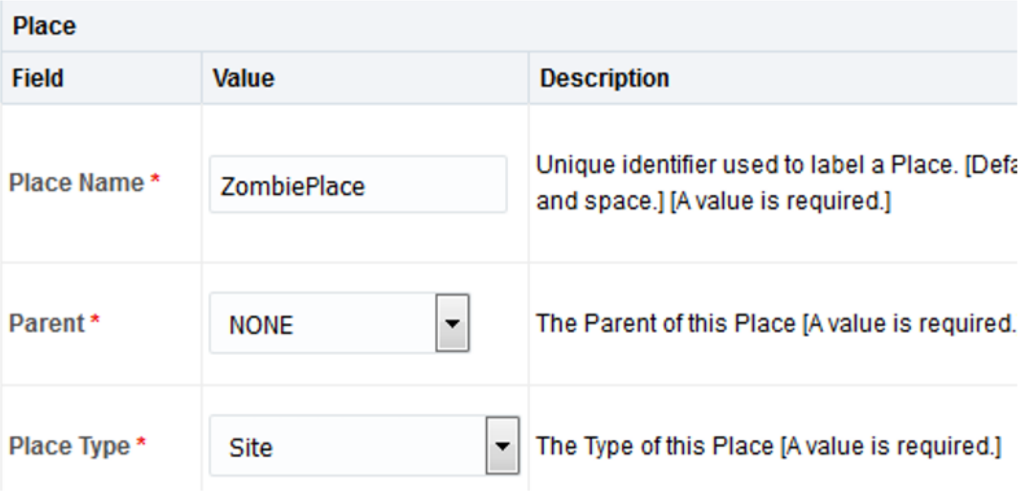
1. In primary NOAM VIP GUI, configure places.

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

   b. Navigate to **Configuration**, and then **Networking**, and then **Places**.

   c. Click **Insert**.

   d. Fill in the fields as follows:



Place

Field	Value	Description
Place Name *	ZombiePlace	Unique identifier used to label a Place. [Defa and space.] [A value is required.]
Parent *	NONE ▾	The Parent of this Place [A value is required.
Place Type *	Site ▾	The Type of this Place [A value is required.]

Place Name:<Site Name>

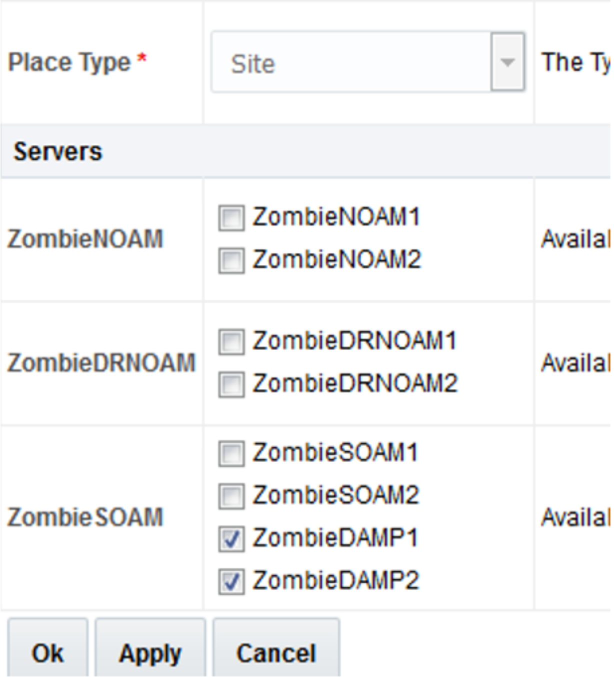
Parent: NONE

Place Type: Site

e. Repeat this step for each of the PCA or DCA Places (Sites) in the network. See the Terminology section for more information on Sites & Places.

2. In NOAM VIP GUI, assign MP server to places.

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



Place Type *	Site ▾	The Ty
Servers		
ZombieNOAM	□ ZombieNOAM1 □ ZombieNOAM2	Availal
ZombieDRNOAM	□ ZombieDRNOAM1 □ ZombieDRNOAM2	Availal
ZombieSOAM	□ ZombieSOAM1 □ ZombieSOAM2 ☑ ZombieDAMP1 ☑ ZombieDAMP2	Availal

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

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

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

Configure the MP Server Group(s) and Profiles

This procedure configures MP server groups.

1. In primary NOAM VIP GUI, enter MP Server Group Data applicable to all C level servers (DAMP, IPFE, VSTP, SBRs).
   a. From the GUI session on the NOAM VIP address, navigate to **Configuration**, and then **Server Groups**.
   b. Click **Insert** and fill out the following fields:
   Server Group Name:[Server Group Name]

   Level: C

   Parent: [SOAM Server Group That is Parent To this MP]

   Function: Select the Proper Function for this MP Server Group:

Table 5-10 MP Server Group

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
IP Front End	IPFE application	1 Active MP Per SG
SBR	Policy and Charging Session/or Policy Binding Function/Universal SBR	1 Active MP, 1 Standby MP, 2 Optional Spare Per SG
STP	vSTP	Multiple vSTP MP per SG
STPService	vSTP	MP for the SMS Home Router feature.

For vSTP:

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

> **Note**
>
> - IPFE interaction with vSTP MP is not supported. There is no support of TSA/Auto selection for vSTP MPs.
> - vSTP MP can co-exist with DA-MP under a SOAM but different server group.
> - vSTP MP requires 8 GB of RAM.
> - vSTP STPService MP must be configured if the SMS Home Router feature is activated by the user after the installation is complete.

For PCA application:

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

  At least one MP Server Group with the **DSR (multi-active cluster**) function must be configured.
- Policy DRA function
  At least two MP Server Groups with the **SBR** function must be configured. One stores session data and one stores binding data.

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

WAN Replication Connection Count:

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

For Policy and Charging Server Groups: 8

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

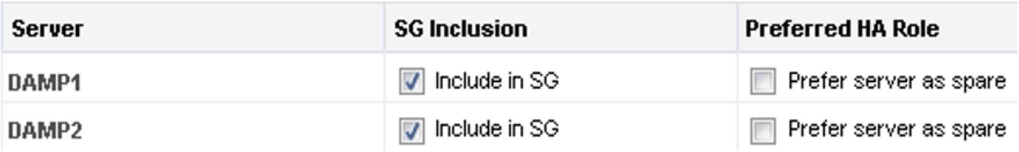
DA-MP (Function: DSR (multi-active cluster))

SBR (Function: SBR)

IPFE (Function: IP Front End)

c. Click **OK** when all fields are filled.

2. In primary NOAM VIP GUI, 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. In primary NOAM VIP GUI, edit the MP server groups to include MPs.
   a. Navigate to **Configuration**, and then **Server Groups**, select a server group that you just created, and click **Edit**.
   b. Select the network element representing the MP server group you wish to edit.
   c. Mark the **Include in SG** checkbox for every MP server you wish to include in this server group. Leave other checkboxes blank.

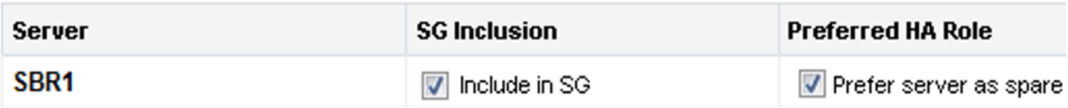


Server	SG Inclusion	Preferred HA Role
DAMP1	☑ Include in SG	□ Prefer server as spare
DAMP2	☑ Include in SG	□ Prefer server as spare

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

   d. Click **OK**.
4. In primary NOAM VIP GUI, edit the MP server group and add preferred spares for site redundancy. This is an optional step, applicable only to PCA.

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.



Server	SG Inclusion	Preferred HA Role
SBR1	☑ Include in SG	☑ Prefer server as spare

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

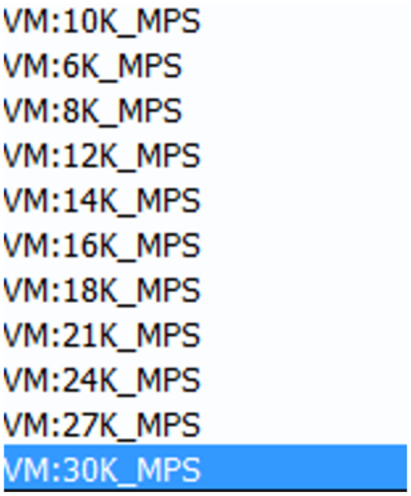
> **Note**
>
> - The preferred spare servers should be different sites from the original server. There should be servers from three separate sites (locations).
> - There must first be non-preferred spare present in the server group before adding the preferred spare.

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

Click **OK** to save.

5. In primary NOAM VIP GUI, repeat steps 1 through 4 for any remaining MP and IPFE server groups you need to create.
6. In primary NOAM VIP GUI, wait for replication to complete on all MPs.
   Wait for the alarm `10200: Remote Database re-initialization in progress` to be cleared and navigate to **Alarms & Events**, and then **Active Alarms**.

   This should happen shortly after you have verified the `Norm` DB status in the previous step.
7. In SOAM VIP GUI, assign profiles to DA-MPs from SOAM GUI.
   a. Log in to the GUI of the active SOAM server as the `guiadmin` user.
   b. From the SO GUI, navigate to **Diameter Common**, and then **MPs**, and then **Profiles Assignments**.
   c. For each MP, select the proper profile assignment based on the MP's type and the function it serves:



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

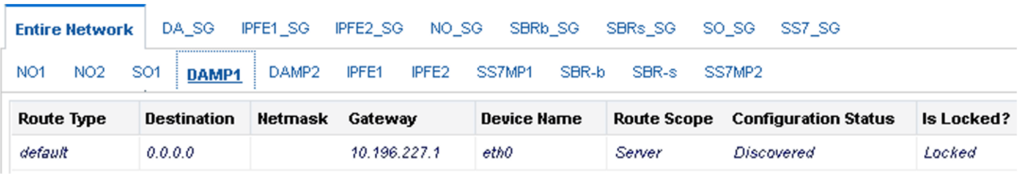
   d. When finished, click **Assign**.

8. In primary NOAM VIP GUI, restart MP VM.
   a. From the NOAM GUI, navigate to **Status & Manage**, and then **Server**.
   b. For each MP server:
      i. Select the MP server.
      ii. Click **Restart**.
      iii. Click **OK** on the confirmation screen. Wait for the message that tells you that the restart was successful.
      Policy and Charging DRA/DCA Installations: You may continue to see alarms related to ComAgent until you complete PCA/DCA installation.

5.1 Configure the Signaling Network Routes

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

1. Establish a GUI session on the NOAM by using the NOAM VIP address. Log in as the `guiadmin` user.
2. In NOAM VIP, navigate to routes configuration screen.
   a. Navigate to **Configuration**, and then **Networking**, and then **Network**, and then **Routes**.
   b. 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.



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. Click **Insert** at the bottom of the screen to add additional routes.

4. In primary NOAM VIP GUI, add default route for MPs going through signaling network gateway.

> **Note**
>
> This is an optional step. Only perform this step if you performed Configure the MP Virtual Machines. That is if you have deleted default XMI route and plan to replace it with default XSI routes.

To delete the existing default route:

a. Log in to the PRIMARY NOAM VIP GUI.

b. Navigate to **Configuration**, and then **Networking**, and then **Networks**.

c. Select the specific SO tab.

d. Select the XMI network and click **Unlock**. Click **OK**.

e. Navigate to **Configuration**, and then **Networking**, and then **Routes**.

f. Select the Specific MP XMI route and click **Delete**.

g. Click **OK**.

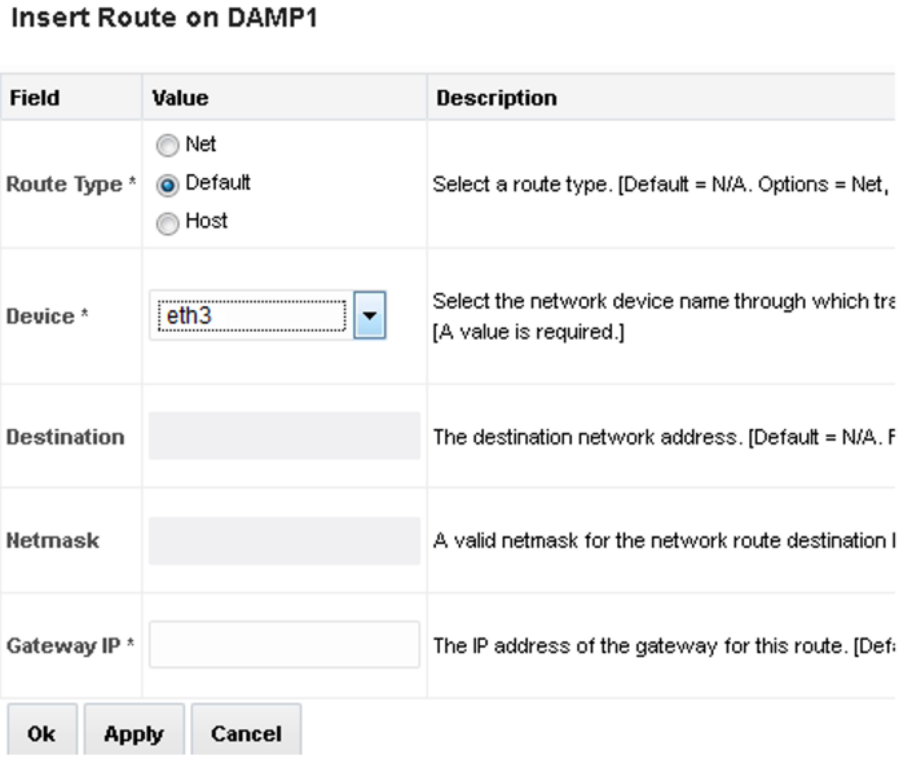
h. Repeat the above steps for all required MPs to delete the XMI routes.

i. Navigate to **Configuration**, and then **Networking**, and then **Networks**.

j. Select the respective SOAM tab.

k. Select the XMI network and click **Lock**.

l. Click **OK**.
If your MP servers no longer have a default route, then you can insert a default route here, which uses one of the signaling network gateways.



Insert Route on DAMP1

Field	Value	Description
Route Type *	○ Net ● Default ○ 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

Route Type: Default

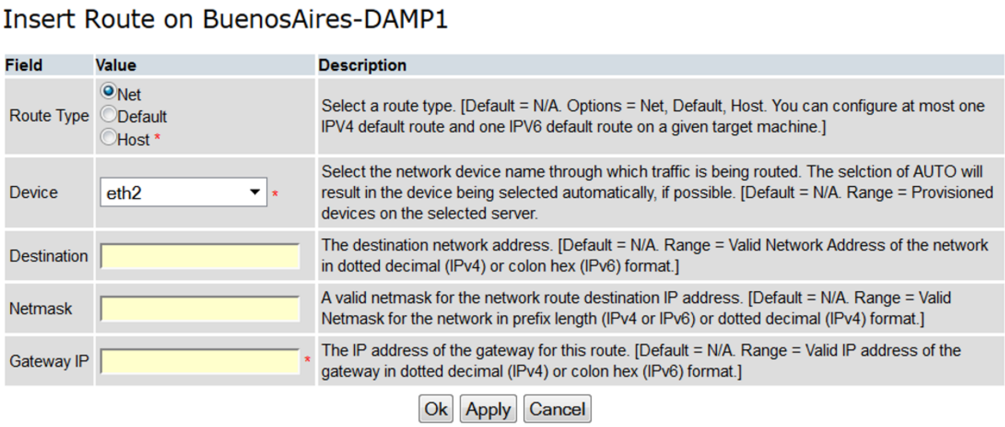
Device: Select the signaling device directly attached to the network where the XSI default gateway resides.

Gateway IP: The XSI gateway you wish to use for default signaling network access.

m. Click **OK**.

5. In primary NOAM VIP GUI, add network routes for diameter peers.

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



Insert Route on BuenosAires-DAMP1

Field	Value	Description
Route Type	● Net ○ Default ○ 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 selction 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.]

Route Type: Net

Device: Select the appropriate signaling interface that is used to connect to that network

Destination: Type the **Network ID** of network to which the peer node is connected to

Netmask: Type the corresponding Netmask

Gateway IP: Type the **IP** of the customer gateway.

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

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

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

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

5.2 Configure DSCP Values for Outgoing Traffic

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.

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

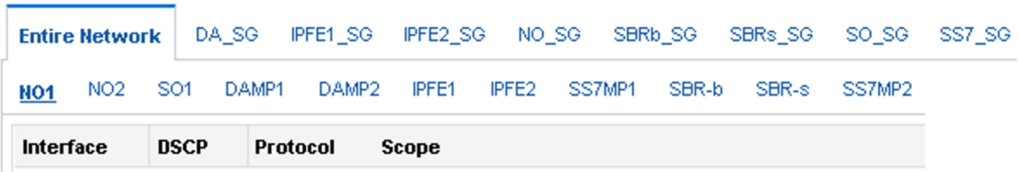
2. In primary NOAM VIP GUI, option 1 is to configure interface DSCP.

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

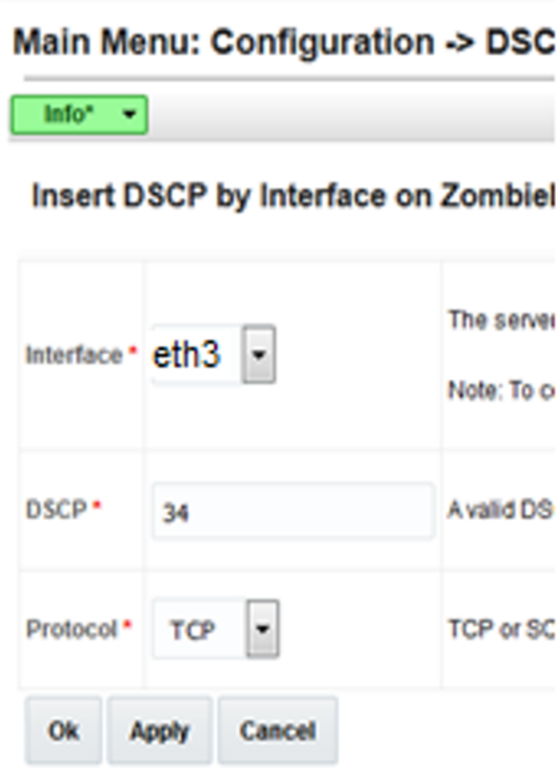
a. Navigate to **Configuration**, and then **Networking**, and then **DSCP**, and then **Interface DSCP**.

b. 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.

c. Click **Insert**.



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



Main Menu: Configuration -> DSC

Insert DSCP by Interface on Zombiel

Interface *	eth3	The serve Note: To c
DSCP *	34	A valid DS
Protocol *	TCP	TCP or SC

e. 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.

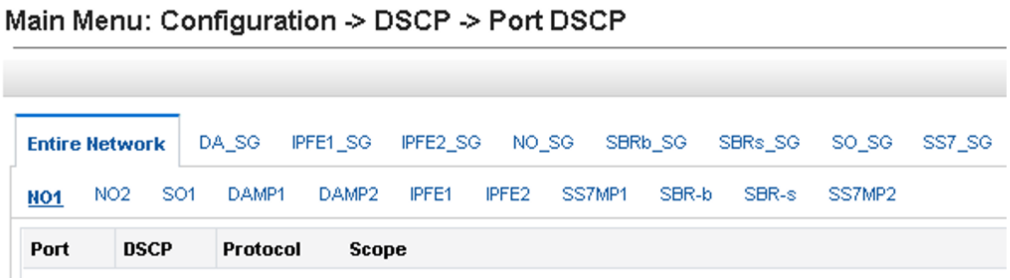
3. In primary NOAM VIP GUI, option 2 is to configure port DSCP.

> **Note**
>
> The values displayed in the screenshots are for demonstration purposes only. The exact DSCP values for your site varies.

a. Navigate to **Configuration**, and then **Networking**, and then **DSCP**, and then **Port DSCP**.

b. 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.

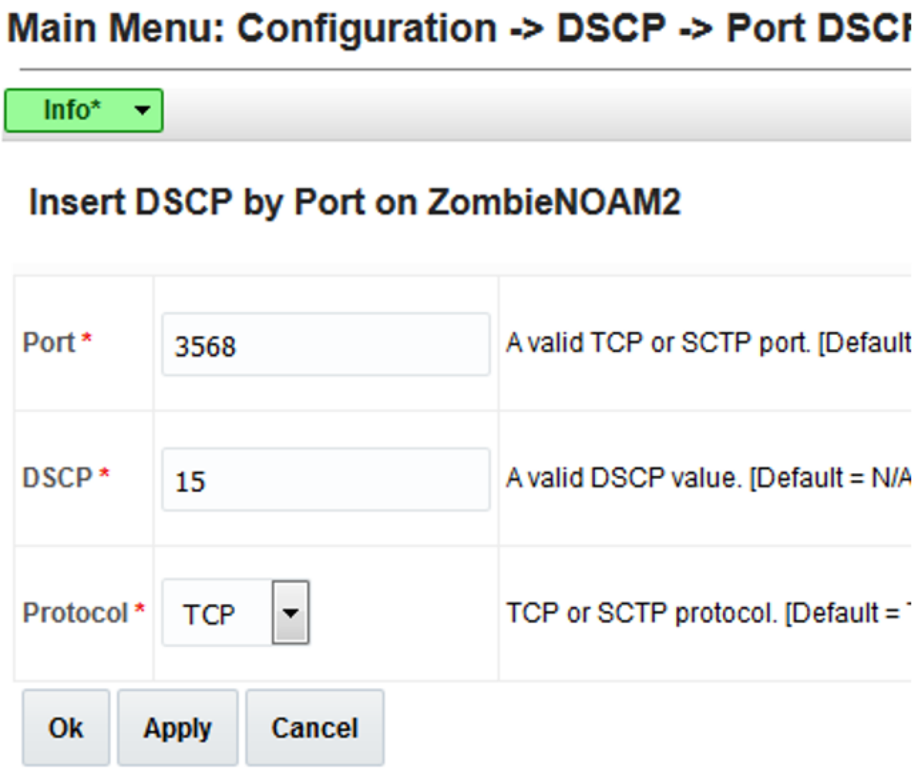
c. Click **Insert**.



Main Menu: Configuration -> DSCP -> Port DSCP

Port	DSCP	Protocol	Scope

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



Main Menu: Configuration -> DSCP -> Port DSCI

Insert DSCP by Port on ZombieNOAM2

Port *	3568	A valid TCP or SCTP port. [Default
DSCP *	15	A valid DSCP value. [Default = N/A
Protocol *	TCP	TCP or SCTP protocol. [Default =

e. 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.

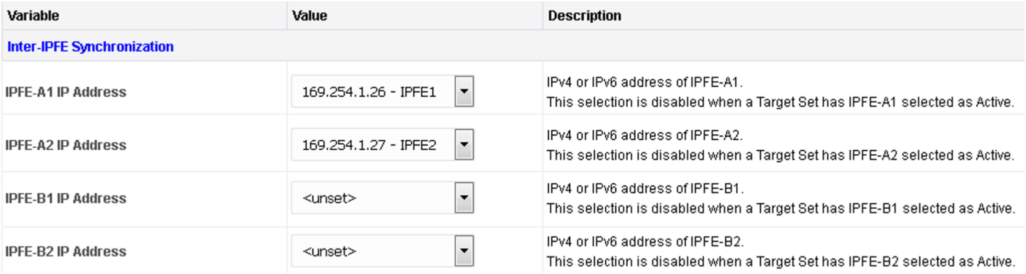
> **Note**
>
> Repeat steps 2-3 for all remaining servers.

5.3 Configure IP Front End

If the DSR guest type is IPFE, see Performance Tuning Recommended .

This procedure configures IP Front End (IPFE) and optimizes performance.

1. Log in to the SOAM VIP GUI as the guiadmin user.
2. In SOAM VIP, configuration of replication IPFE association data.
   a. Navigate to **IPFE**, and then **Configuration**, and then **Options**.
   b. 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.
   c. If applicable, type the address of the 3rd and 4th IPFE servers in **IPFE-B1 IP Address** and **IPFE-B2 IP Address** fields.



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.

> **Note**
>
> - It is recommended that the address resides on the **IMI (Internal Management Interface)** network.
> - **IPFE-A1** and **IPFE-A2** must have connectivity between each other using these addresses. The same applies to **IPFE-B1** and **IPFE-B2**.

3. In SOAM VIP, configuration of IPFE target sets (Part 1).

   a. Log into the SOAM VIP GUI as the `guiadmin` user.

   b. Navigate to **IPFE**, and then **Configuration**, and then **Target Sets**.

   c. Click either **Insert IPv4** or **Insert IPv6** depending on the IP version of the target set you plan to use.
   This screen displays the following configurable settings:

   Protocols: Protocols the target set supports.

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

   Load Balance Algorithm: Hash or Least Load options.

> **Note**
>
> - For the IPFE to provide Least Load distribution, navigate to **IPFE**, and then **Configuration**, and then **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.
> - The Least Load option is the default setting, and is the recommended option with exception of unique backward compatibility scenarios.

4. In SOAM VIP, configuration of IPFE target sets (Part 2).

   a. Navigate to **IPFE**, and then **Configuration**, and then **Target Sets**.
   (Optional): If you have selected the **Least Load** algorithm, then you may configure the following fields to adjust the algorithm’s behavior:

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

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

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

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

> ⓘ **Note**
>
> This address must reside on the XSI (External Signaling Interface) network because it is used by the application clients to reach the application servers. This address must not be a real interface address (that is, must not be associated with a network interface card).

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

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

> ⓘ **Note**
>
> - A secondary address is required to support SCTP multi-homing. A secondary address can support TCP, but the TCP connections are not multi-homed.
> - If SCTP multi-homing is to be supported, select the mate IPFE of the Active IPFE for the Active IPFE for secondary address to ensure SCTP failover functions as designed.

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

> **Note**
>
> - – The IP address must be on the XSI network since they must be on the same network as the target set address. This address must also match the IP version of the target set address (IPv4 or IPv6). If the Secondary Public IP Address is configured, it must reside on the same application server as the first IP address.
>   – A port must be created to associate the IP that needs to be used as TSA IP in cloud. Create a port using the following command:
>
>   ```
>   neutron port-create <xsi network-id>
>   ```
>
>   The command results in an IP that can be used as TSA IP.
>   – If all application servers have an equal weight (for example, 100, which is the default), they have an equal chance of being selected. Application servers with larger weights have a greater chance of being selected.

b. Click **Add** to add more application servers (up to 16).

c. Click **Apply**.

5. In SOAM VIP, repeat for additional configuration of IPFE target sets.

   Repeat steps 3 and 4 for each target set (up to 16).
   At least one target set must be configured.

5.4 Configure the Desired MTU value

By default DSR defines MTU size of all its management and/or signaling networks as 1500 bytes. If the configured virtual network(s) on cloud is VXLAN based and MTU size defined/ negotiated on it is 1500 bytes, then we need to accommodate VXLAN header (size 65 bytes) within these 1500 bytes.
This procedure configures the desired MTU value.

1. Verify the MTU on DSR system, by running the following command:

   ```
   iqt -pE NetworkDeviceOption
   ```

   Sample output:

   ```
   DeviceOption_ID=0 Keyword=MTU Device_ID=0 Value=1500
   DeviceOption_ID=1 Keyword=bootProto Device_ID=0 Value=none
   DeviceOption_ID=2 Keyword=onboot Device_ID=0 Value=yes
   DeviceOption_ID=3 Keyword=MTU Device_ID=1 Value=1500
   DeviceOption_ID=4 Keyword=bootProto Device_ID=1 Value=none
   DeviceOption_ID=5 Keyword=onboot Device_ID=1 Value=yes
   DeviceOption_ID=6 Keyword=MTU Device_ID=2 Value=1500
   DeviceOption_ID=7 Keyword=bootProto Device_ID=2 Value=none
   DeviceOption_ID=8 Keyword=onboot Device_ID=2 Value=yes
   DeviceOption_ID=9 Keyword=MTU Device_ID=3 Value=1500
   DeviceOption_ID=10 Keyword=bootProto Device_ID=3 Value=none
   DeviceOption_ID=11 Keyword=onboot Device_ID=3 Value=yes
   ```

```
DeviceOption_ID=12 Keyword=MTU Device_ID=4 Value=1500
DeviceOption_ID=13 Keyword=bootProto Device_ID=4 Value=none
DeviceOption_ID=14 Keyword=onboot Device_ID=4 Value=yes
```

2. Change the MTU value on DSR system.

   This is an optional step.
   If the MTU value is 1500 bytes, change it to 1435 bytes, by executing:

   ```
   sudo iset -fValue=1435 NetworkDeviceOption where “Keyword='MTU'”
   === changed 256 records ===
   ```

   Wait for few minutes.

3. Verify the MTU value on DSR system by running the following command:

   ```
   ip addr
   ```

   Sample output:

   ```
   1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN link/
   loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 inet 127.0.0.1/8 scope
   host lo inet6 ::1/128 scope host valid_lft forever preferred_lft forever
   2: control: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast
   state UP qlen 1000 link/ether 02:79:b5:f7:65:0e brd ff:ff:ff:ff:ff:ff inet
   192.168.1.32/24 brd 192.168.1.255 scope global control inet6
   fe80::79:b5ff:fef7:650e/64 scope link valid_lft forever preferred_lft
   forever
   3: xmi: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1435 qdisc pfifo_fast state
   UP qlen 1000 link/ether 02:90:04:c6:3b:e1 brd ff:ff:ff:ff:ff:ff inet
   10.75.198.37/25 brd 10.75.198.127 scope global xmi inet 10.75.198.4/25
   scope global secondary xmi inet6 2606:b400:605:b821:90:4ff:fec6:3be1/64
   scope global dynamic valid_lft 2591870sec preferred_lft 604670sec inet6
   fe80::90:4ff:fec6:3be1/64 scope link valid_lft forever preferred_lft
   forever
   4: imi: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1435 qdisc pfifo_fast state
   UP qlen 1000 link/ether 02:3b:48:96:3c:61 brd ff:ff:ff:ff:ff:ff inet
   192.168.100.32/24 brd 192.168.100.255 scope global imi inet6
   fe80::3b:48ff:fe96:3c61/64 scope link valid_lft forever preferred_lft
   forever
   ```

   Verify on all nodes:

   ```
   iqt -pE NetworkDeviceOption
   ```

   Sample output:

   ```
   DeviceOption_ID=0 Keyword=MTU Device_ID=0 Value=1435
   DeviceOption_ID=1 Keyword=bootProto Device_ID=0 Value=none
   DeviceOption_ID=2 Keyword=onboot Device_ID=0 Value=yes
   DeviceOption_ID=3 Keyword=MTU Device_ID=1 Value=1435
   DeviceOption_ID=4 Keyword=bootProto Device_ID=1 Value=none
   DeviceOption_ID=5 Keyword=onboot Device_ID=1 Value=yes
   DeviceOption_ID=6 Keyword=MTU Device_ID=2 Value=1435
   ```

```
DeviceOption_ID=7 Keyword=bootProto Device_ID=2 Value=none
DeviceOption_ID=8 Keyword=onboot Device_ID=2 Value=yes
DeviceOption_ID=9 Keyword=MTU Device_ID=3 Value=1435
DeviceOption_ID=10 Keyword=bootProto Device_ID=3 Value=none
DeviceOption_ID=11 Keyword=onboot Device_ID=3 Value=yes
DeviceOption_ID=12 Keyword=MTU Device_ID=4 Value=1435
DeviceOption_ID=13 Keyword=bootProto Device_ID=4 Value=none
DeviceOption_ID=14 Keyword=onboot Device_ID=4 Value=yes
```

5.5 IDIH Deployment Using VNFM

For IDIH 9.2 installation, refer *Oracle CommunicationsVirtual Network Functions Manager Installation and User Guide* 6.2 version.

5.5.1 IDIH Deployment on KVM with RAW Images

Perform the following procedure to set up the VMs (Virtual Machine):

1. Log in to KVM host machine.
2. Navigate to a directory where enough space is available.
   Refer the following table for flavors:

Table 5-11 IDIH Flavor Value

Flavor Name	VCPUs	RAM(GB)	Root Disk(GB)	Ephemeral	Swap Disk
kafka_flavor	6	16	170	0	0
Mysql-DB-DataNode	6	16	220	0	0
service_profile	6	16	120	0	0

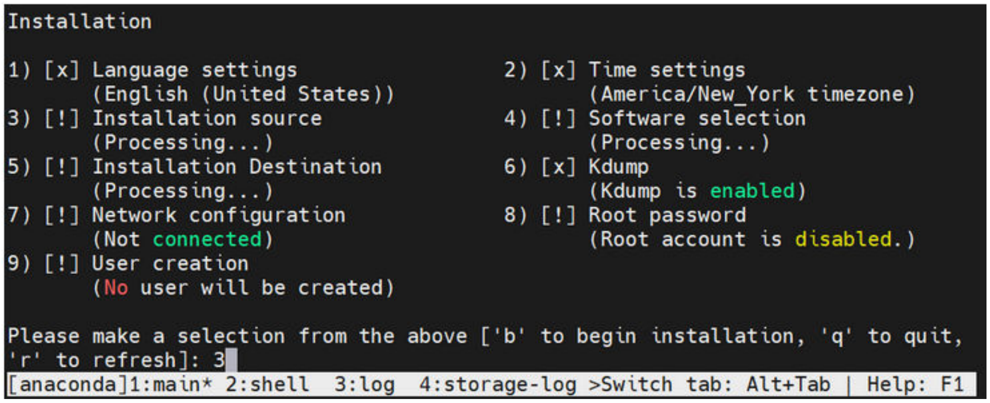
3. Create empty qcow2 image files for MySQL, Kafka, and services.
   a. `qemu-img create -f qcow2 idih-mysql.qcow2 220G`
   b. `qemu-img create -f qcow2 idih-kafka.qcow2 170G`
   c. `qemu-img create -f qcow2 idih-service.qcow2 120G`
4. Copy the `OracleLinux-R8-U9-x86_64-dvd.iso` file to host machine.
5. Create MySQL VM, Kafka VM, and Service VM by running the following commands on host machine.

```
virt-install \
  --name idih-mysql \
  --ram 16384 \
  --vcpus 6 \
  --disk path=idih-mysql.qcow2,size=220,format=qcow2 \
  --os-type linux \
  --os-variant ol8.0 \
  --network network=default \
  --graphics none \
  --location OracleLinux-R8-U10-x86_64-dvd.iso \
  --extra-args 'console=ttyS0'
```

```
virt-install \
--name idih-kafka \
--ram 16384 \
--vcpus 6 \
--disk path=idih-kafka.qcow2,size=170,format=qcow2 \
--os-type linux \
--os-variant ol8.0 \
--network network=default \
--graphics none \
--location OracleLinux-R8-U10-x86_64-dvd.iso \
--extra-args 'console=ttyS0'

  virt-install \
--name idih-service \
--ram 16384 \
--vcpus 6 \
--disk path=idih-service.qcow2,size=120,format=qcow2 \
--os-type linux \
--os-variant ol8.0 \
--network network=default \
--graphics none \
--location OracleLinux-R8-U10-x86_64-dvd.iso \
--extra-args 'console=ttyS0'
```

> **Note**
>
> The installation process is interactive, and the user must complete all the steps marked with [!] by selecting the options one at a time.

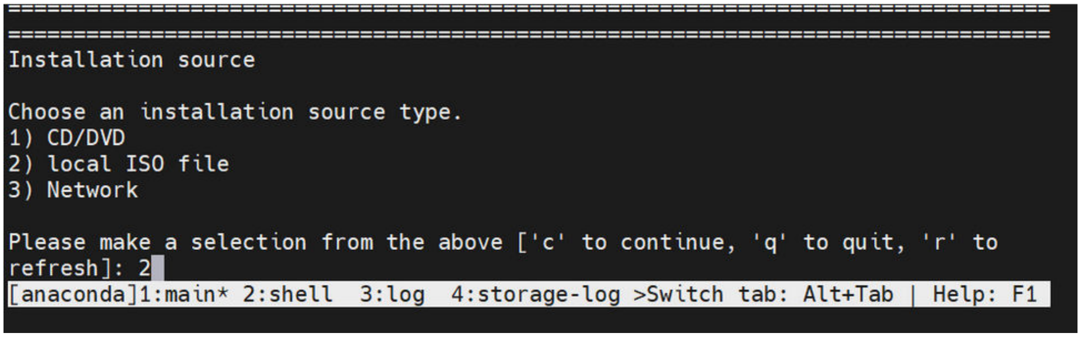
Figure 5-1 Installation



```
Installation

1) [x] Language settings                 2) [x] Time settings
       (English (United States))                (America/New_York timezone)
3) [!] Installation source               4) [!] Software selection
       (Processing...)                          (Processing...)
5) [!] Installation Destination          6) [x] Kdump
       (Processing...)                          (Kdump is enabled)
7) [!] Network configuration             8) [!] Root password
       (Not connected)                          (Root account is disabled.)
9) [!] User creation
       (No user will be created)

Please make a selection from the above ['b' to begin installation, 'q' to quit,
'r' to refresh]: 3
[anaconda]1:main* 2:shell  3:log  4:storage-log >Switch tab: Alt+Tab | Help: F1
```

6. Select a source type from the following installation sources:
   - CD/DVD
   - Local ISO file
   - Network

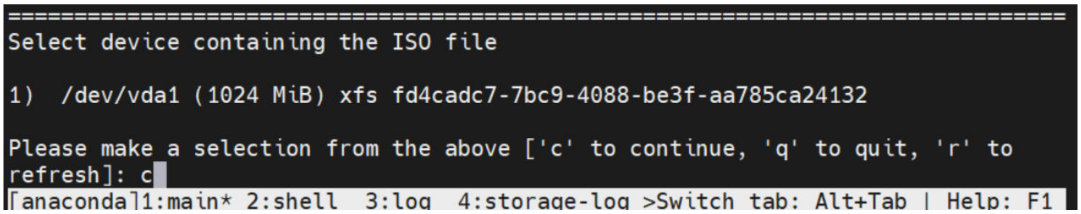
Figure 5-2 Installation Source



```
================================================================================
================================================================================
Installation source

Choose an installation source type.
1) CD/DVD
2) local ISO file
3) Network

Please make a selection from the above ['c' to continue, 'q' to quit, 'r' to
refresh]: 2
[anaconda]1:main* 2:shell  3:log  4:storage-log >Switch tab: Alt+Tab | Help: F1
```

7. Select a device containing the ISO file. After selection of ISO file, the installation process initiates.

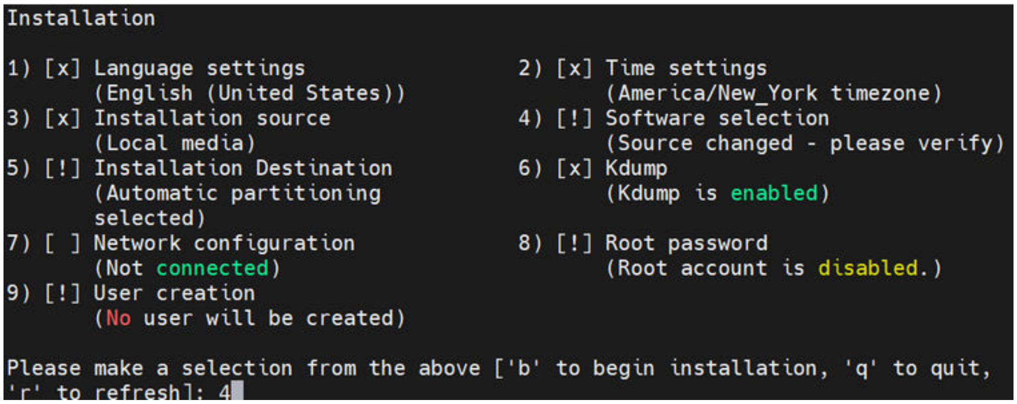
Figure 5-3 ISO File



```
================================================================================
Select device containing the ISO file

1)  /dev/vda1 (1024 MiB) xfs fd4cadc7-7bc9-4088-be3f-aa785ca24132

Please make a selection from the above ['c' to continue, 'q' to quit, 'r' to
refresh]: c
[anaconda]1:main* 2:shell  3:log  4:storage-log >Switch tab: Alt+Tab | Help: F1
```

8. Wait for the processing to complete. Press "r" to refresh and check if step 3 is completed before proceeding to step 4.

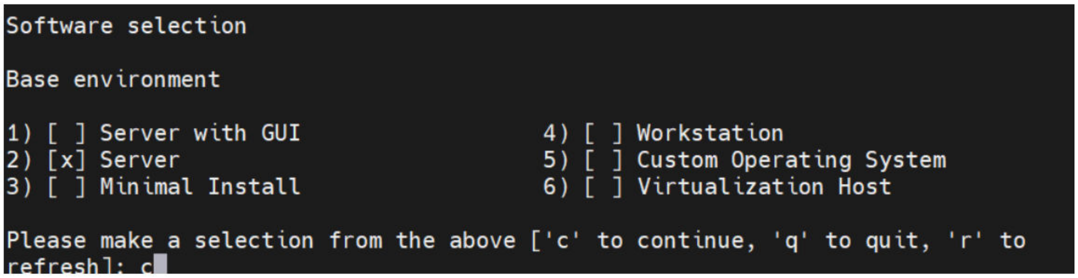
Figure 5-4 Installation process



```
Installation

1) [x] Language settings                 2) [x] Time settings
       (English (United States))                (America/New_York timezone)
3) [x] Installation source               4) [!] Software selection
       (Local media)                            (Source changed - please verify)
5) [!] Installation Destination          6) [x] Kdump
       (Automatic partitioning                  (Kdump is enabled)
       selected)
7) [ ] Network configuration             8) [!] Root password
       (Not connected)                          (Root account is disabled.)
9) [!] User creation
       (No user will be created)

Please make a selection from the above ['b' to begin installation, 'q' to quit,
'r' to refresh]: 4
```

9. Select a software from the following base environment:
   a. Server with GUI
   b. Server
   c. Minimal Install
   d. Workstation
   e. Custom Operating System
   f. Virtualization Host

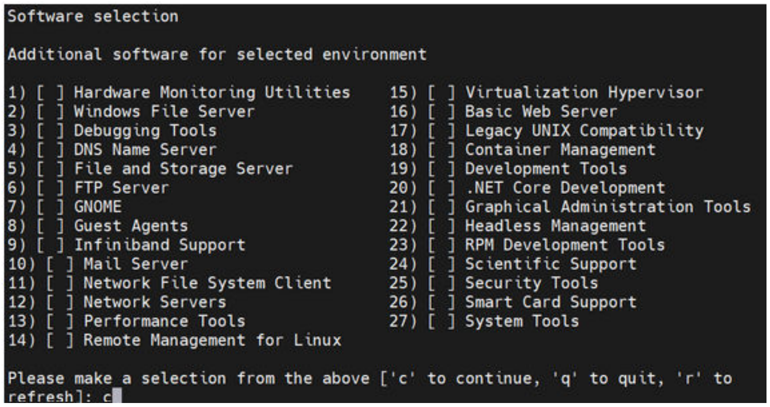
Figure 5-5 Software Selection



```
Software selection

Base environment

1) [ ] Server with GUI                  4) [ ] Workstation
2) [x] Server                           5) [ ] Custom Operating System
3) [ ] Minimal Install                  6) [ ] Virtualization Host

Please make a selection from the above ['c' to continue, 'q' to quit, 'r' to
refresh]: c
```

10. Select **Additional Software** for the selected environment:

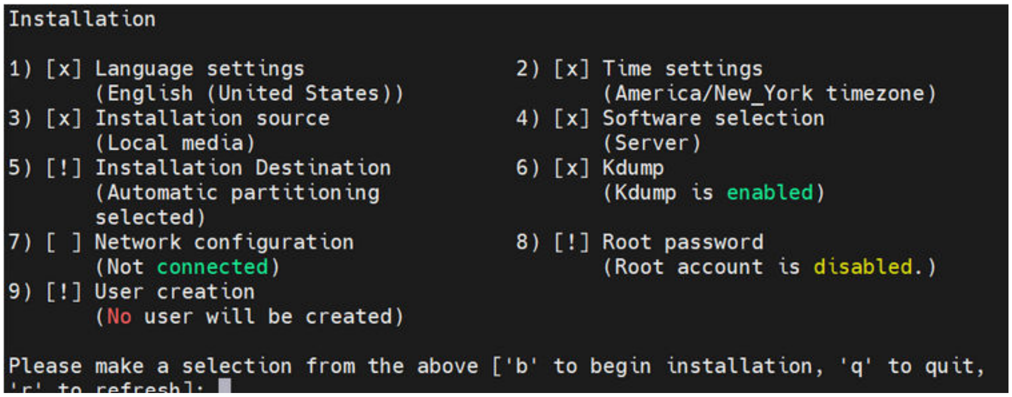
Figure 5-6 Additional Software



```
Software selection

Additional software for selected environment

1) [ ] Hardware Monitoring Utilities    15) [ ] Virtualization Hypervisor
2) [ ] Windows File Server              16) [ ] Basic Web Server
3) [ ] Debugging Tools                  17) [ ] Legacy UNIX Compatibility
4) [ ] DNS Name Server                  18) [ ] Container Management
5) [ ] File and Storage Server          19) [ ] Development Tools
6) [ ] FTP Server                       20) [ ] .NET Core Development
7) [ ] GNOME                            21) [ ] Graphical Administration Tools
8) [ ] Guest Agents                     22) [ ] Headless Management
9) [ ] Infiniband Support               23) [ ] RPM Development Tools
10) [ ] Mail Server                     24) [ ] Scientific Support
11) [ ] Network File System Client      25) [ ] Security Tools
12) [ ] Network Servers                 26) [ ] Smart Card Support
13) [ ] Performance Tools               27) [ ] System Tools
14) [ ] Remote Management for Linux

Please make a selection from the above ['c' to continue, 'q' to quit, 'r' to
refresh]: c
```

11. Wait a moment for the processing to complete, then press "r" to refresh and confirm that step 4 is marked as complete.

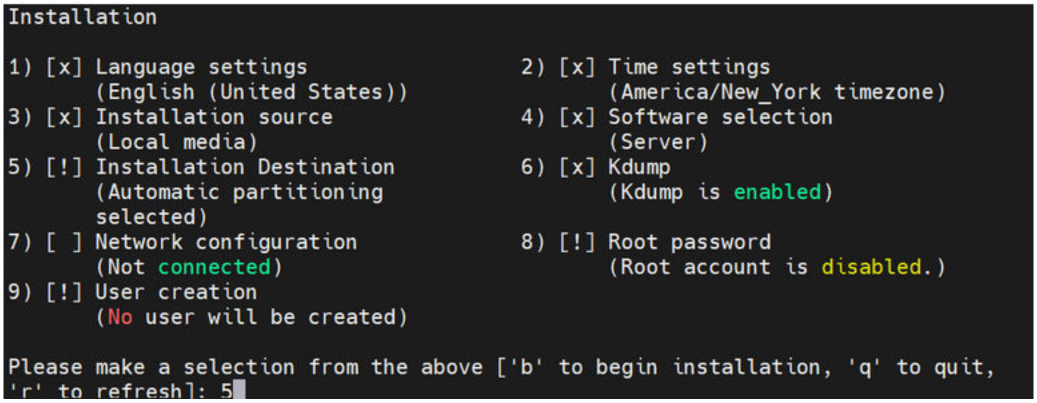
Figure 5-7 Installation



```
Installation

1) [x] Language settings                 2) [x] Time settings
       (English (United States))                (America/New_York timezone)
3) [x] Installation source               4) [x] Software selection
       (Local media)                            (Server)
5) [!] Installation Destination          6) [x] Kdump
       (Automatic partitioning                  (Kdump is enabled)
       selected)
7) [ ] Network configuration             8) [!] Root password
       (Not connected)                          (Root account is disabled.)
9) [!] User creation
       (No user will be created)

Please make a selection from the above ['b' to begin installation, 'q' to quit,
'r' to refresh]:
```

12. Proceed with the next steps, and once all the steps are marked with [x], press "b" to start the installation.

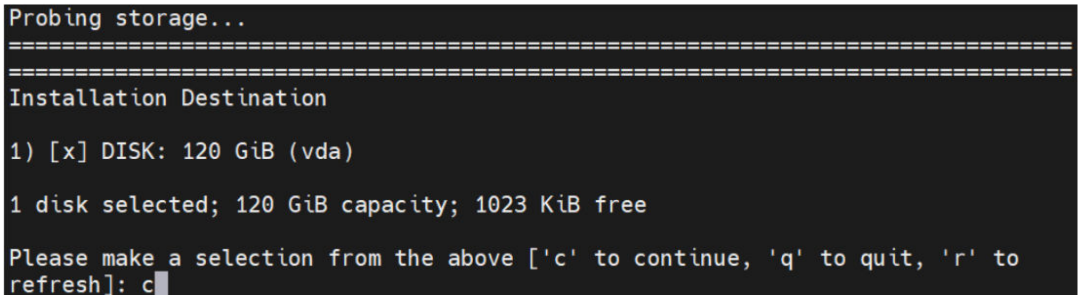
Figure 5-8 Installation



```
Installation

1) [x] Language settings                 2) [x] Time settings
       (English (United States))                (America/New_York timezone)
3) [x] Installation source               4) [x] Software selection
       (Local media)                            (Server)
5) [!] Installation Destination          6) [x] Kdump
       (Automatic partitioning                  (Kdump is enabled)
       selected)
7) [ ] Network configuration             8) [!] Root password
       (Not connected)                          (Root account is disabled.)
9) [!] User creation
       (No user will be created)

Please make a selection from the above ['b' to begin installation, 'q' to quit,
'r' to refresh]: 5
```

Installation Destination is selected during the probing storage.

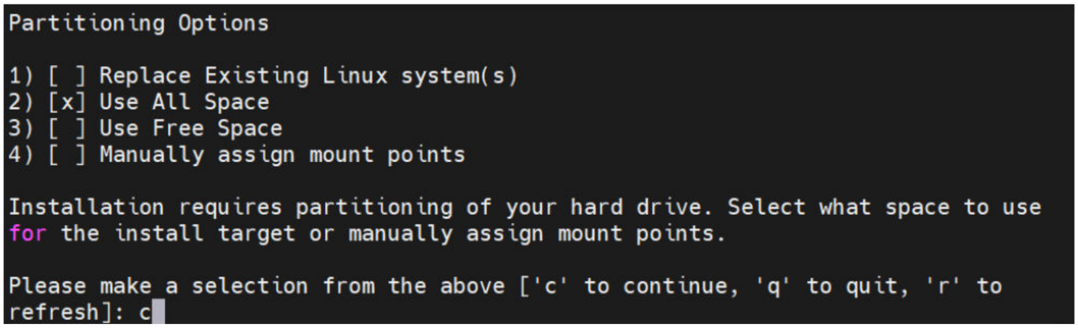
Figure 5-9 Probing storage



```
Probing storage...
================================================================================
================================================================================
Installation Destination

1) [x] DISK: 120 GiB (vda)

1 disk selected; 120 GiB capacity; 1023 KiB free

Please make a selection from the above ['c' to continue, 'q' to quit, 'r' to
refresh]: c
```

13. For partitioning options, select the space to be used for the install target or manually assign mount points.

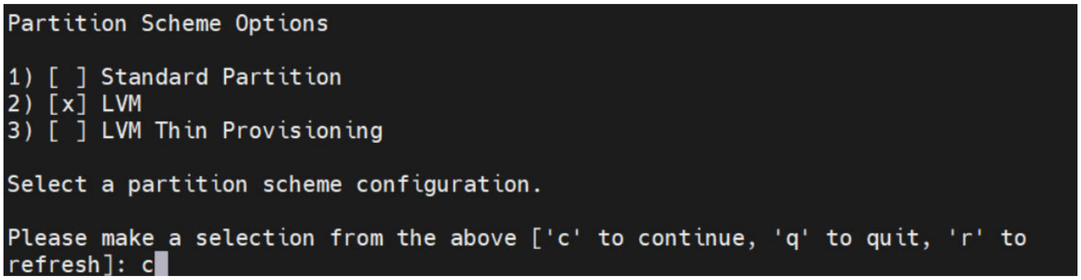
Figure 5-10 Partitioning Options



```
Partitioning Options

1) [ ] Replace Existing Linux system(s)
2) [x] Use All Space
3) [ ] Use Free Space
4) [ ] Manually assign mount points

Installation requires partitioning of your hard drive. Select what space to use
for the install target or manually assign mount points.

Please make a selection from the above ['c' to continue, 'q' to quit, 'r' to
refresh]: c
```

14. Select a Partition Scheme Configuration from the following options:
    a. Standard Partition
    b. LVM
    c. LVM Thin Provisioning

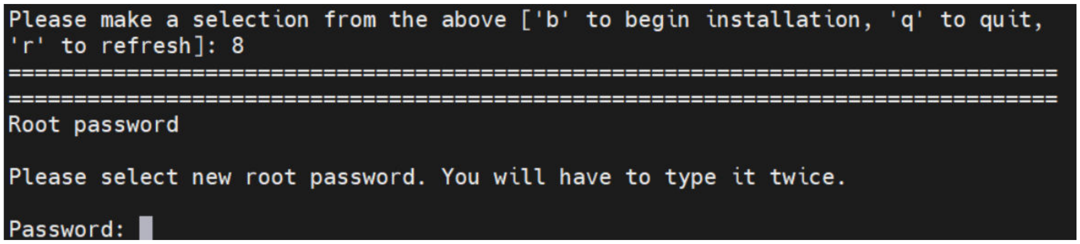
Figure 5-11 Partitioning Scheme Options



```
Partition Scheme Options

1) [ ] Standard Partition
2) [x] LVM
3) [ ] LVM Thin Provisioning

Select a partition scheme configuration.

Please make a selection from the above ['c' to continue, 'q' to quit, 'r' to
refresh]: c
```

15. Set a strong password for the root user and confirm.

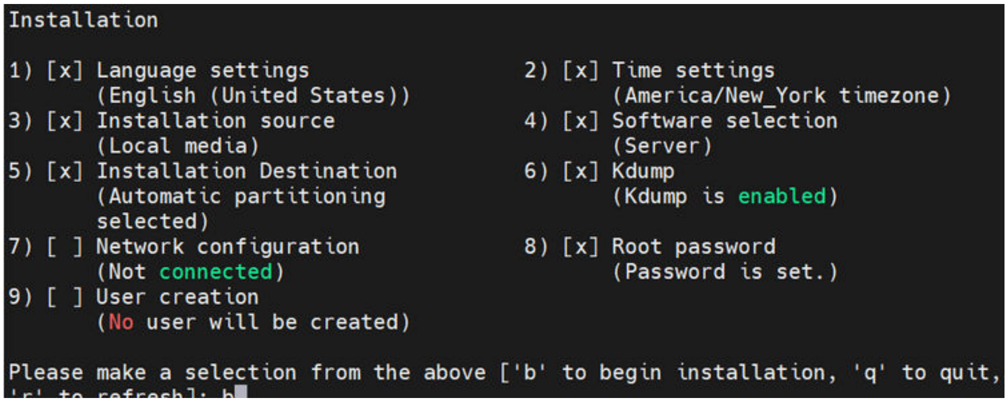
Figure 5-12 Set password for root user



```
Please make a selection from the above ['b' to begin installation, 'q' to quit,
'r' to refresh]: 8
================================================================================
================================================================================
Root password

Please select new root password. You will have to type it twice.

Password:
```

After selection of the password, the installation procedure initiates.

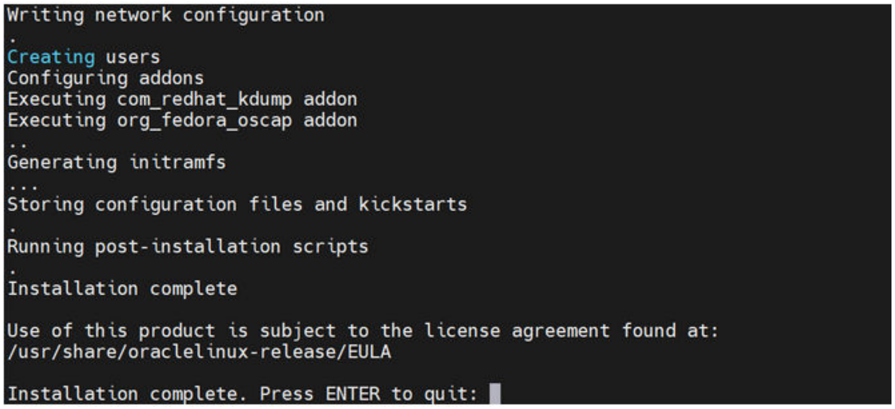
Figure 5-13 Begin Installation



```
Installation

1) [x] Language settings                     2) [x] Time settings
       (English (United States))                    (America/New_York timezone)
3) [x] Installation source                   4) [x] Software selection
       (Local media)                                (Server)
5) [x] Installation Destination              6) [x] Kdump
       (Automatic partitioning                      (Kdump is enabled)
       selected)
7) [ ] Network configuration                 8) [x] Root password
       (Not connected)                              (Password is set.)
9) [ ] User creation
       (No user will be created)

Please make a selection from the above ['b' to begin installation, 'q' to quit,
'r' to refresh]: b
```

Writing network configuration in progress.

Figure 5-14 Writing network configuration



```
Writing network configuration
.
Creating users
Configuring addons
Executing com_redhat_kdump addon
Executing org_fedora_oscap addon
..
Generating initramfs
...
Storing configuration files and kickstarts
.
Running post-installation scripts
.
Installation complete

Use of this product is subject to the license agreement found at:
/usr/share/oraclelinux-release/EULA

Installation complete. Press ENTER to quit:
```

16. Press Enter Key to quit.
17. User must add 3 network interfaces for each VM, xmi, imi, and xsi. Shut down the VM and follow the following steps if you encounter a "No PCI slots available" error while adding any interface.

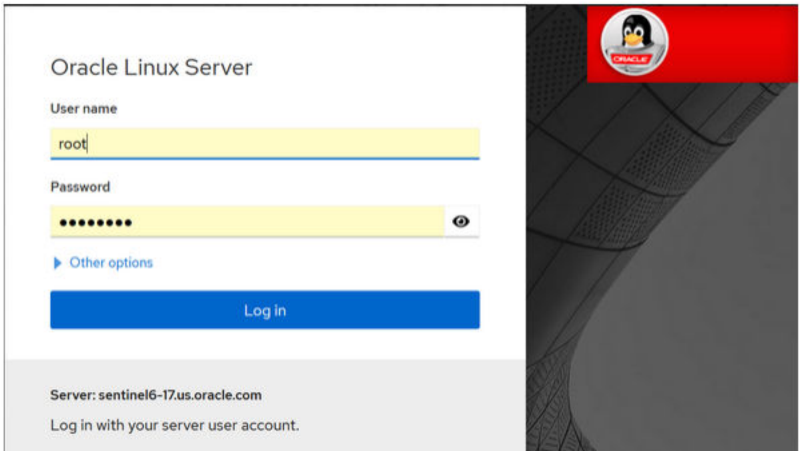
> **Note**
>
> This step is optional, user must add controller only if they encounter "No PCI slots available"error while adding an interface.

18. Run the following command to add the controller:

```
virsh edit <vm-name> and add below controller after index=7

<controller type='pci' index='8' model='pcie-root-port'>
      <model name='pcie-root-port'/>
      <target chassis='8' port='0xf'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01'
function='0x7'/>
</controller>
```

19. Turn on the VM after controller is added.
20. Log in to the host machine with a valid username and password.

Figure 5-15 Login Page



Oracle Linux Server

User name: root

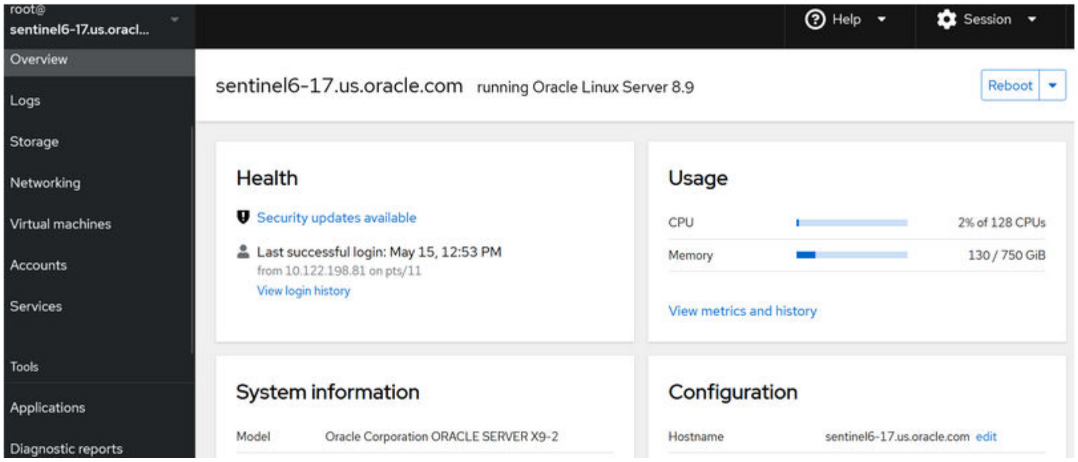
Password: ••••••••

Server: sentinel6-17.us.oracle.com

Log in with your server user account.

After signing in, the system will automatically open the Overview page.

Figure 5-16 Overview



sentinel6-17.us.oracle.com running Oracle Linux Server 8.9

Health

Security updates available

Last successful login: May 15, 12:53 PM
from 10.122.198.81 on pts/11
View login history

Usage

CPU 2% of 128 CPUs
Memory 130 / 750 GiB

View metrics and history

System information

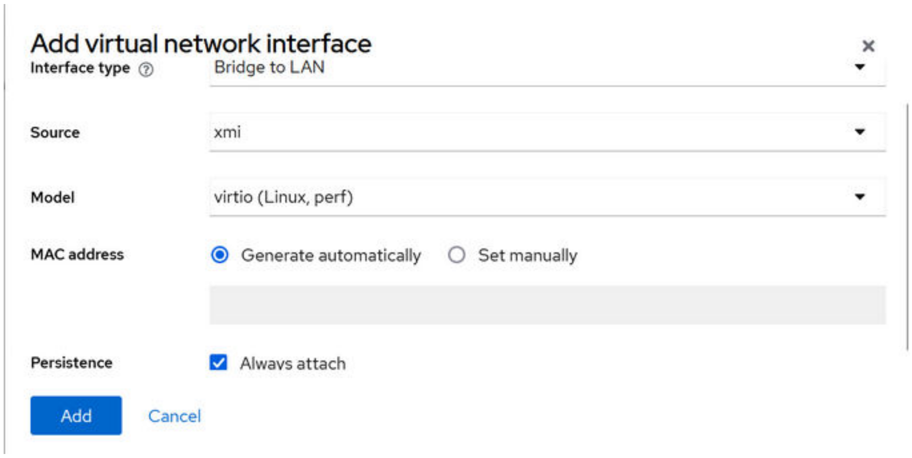
Model Oracle Corporation ORACLE SERVER X9-2

Configuration

Hostname sentinel6-17.us.oracle.com edit

21. Click **Virtual machines** and search for the `idih-mysql` VM. Go to **Network interfaces** section, click **Add Network Interface**, select value as shown in the following screenshot, and click **Add**.

Figure 5-17   Add Virtual Network Interface



Add virtual network interface

Interface type: Bridge to LAN

Source: xmi

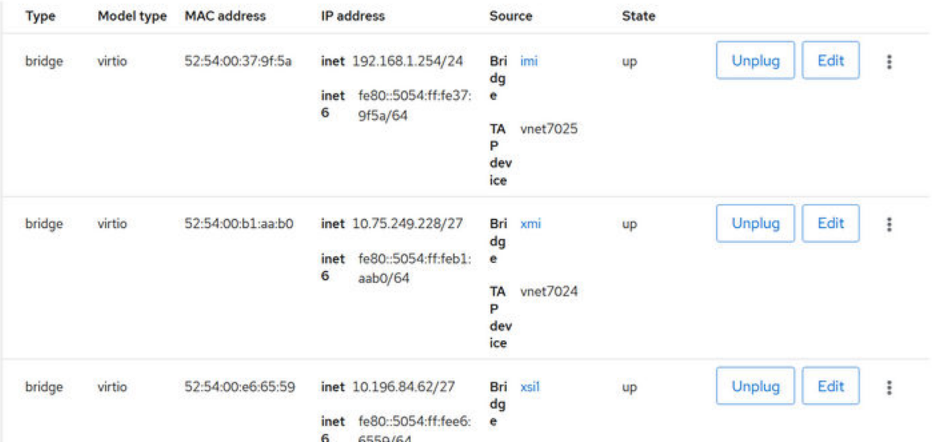
Model: virtio (Linux, perf)

MAC address: ● Generate automatically ○ Set manually

Persistence: ☑ Always attach

22. Apply the same process to the IMI and XSI interfaces. The following screenshot displays all the interfaces.

Figure 5-18   Interfaces



Type	Model type	MAC address	IP address	Source	State
bridge	virtio	52:54:00:37:9f:5a	inet 192.168.1.254/24 inet6 fe80::5054:ff:fe37:9f5a/64	Bridge imi TAP device vnet7025	up
bridge	virtio	52:54:00:b1:aa:b0	inet 10.75.249.228/27 inet6 fe80::5054:ff:feb1:aab0/64	Bridge xmi TAP device vnet7024	up
bridge	virtio	52:54:00:e6:65:59	inet 10.196.84.62/27 inet6 fe80::5054:ff:fee6:6559/64	Bridge xsil	up

23. Log in to the VM through CLI. You can change the hostname of the VM by editing the following command. Provide a name of your preference.

```
- vi /etc/hostname
```

24. Assign a valid IP address for all the three interfaces for the three VMs created.

25. Run `ifconfig` command and take a note of device names -enp1s0, enp7s0, and enp8s0. Here, enp1s0 represents xmi, enp7s0 represents imi, and enp8s0 represents xsi.

26. Run the following command, it will display the status as "disconnected" for all the interfaces.

```
nmcli dev status
```

27. To assign an IP addresss to enp1s0, run the following command:

```
nmcli con edit enp1s0
```

If you get an error, then most likely the device is not up. You can bring it up by running the following command:

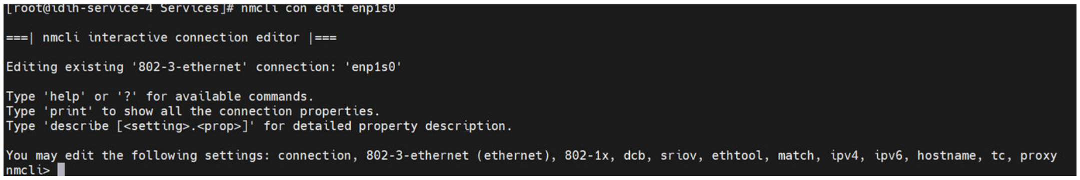
```
nmcli dev up enp1s0
```

.

28. After the device is up, re-run the following command. Prompt must be visible as shown in the below screenshot:

```
nmcli con edit enp1s0. nmcli
```

Figure 5-19 Prompt



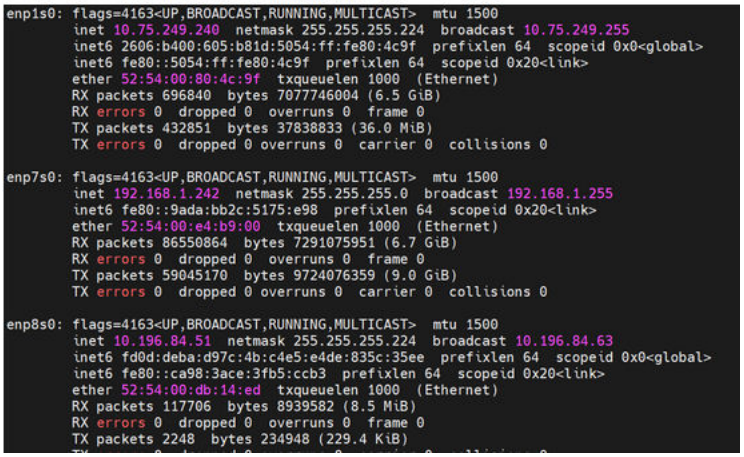
```
[root@idih-service-4 Services]# nmcli con edit enp1s0

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'enp1s0'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, ethtool, match, ipv4, ipv6, hostname, tc, proxy
nmcli>
```

   a. Perform the following steps to assign the IP address to `enp1s0`:
      i. Set ipv4.addresses <ip-address>
      ii. set ipv4.gateway <gateway-ip>
      iii. Save and quit.
   b. You can type print in `nmcli` prompt to verify the assigned IP.
   c. Apply the same steps for enp7s0 and enp8s0 interfaces.

29. Ensure that `onboot=yes` in the following `/etc/sysconfig/network-scripts/ifcfg-enp1s0` ile.

30. Restart the VM and check if IP addresses are assigned with help of `ifconfig`.

Figure 5-20 ifconfig



```
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.75.249.240  netmask 255.255.255.224  broadcast 10.75.249.255
        inet6 2606:b400:605:b81d:5054:ff:fe80:4c9f  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::5054:ff:fe80:4c9f  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:80:4c:9f  txqueuelen 1000  (Ethernet)
        RX packets 696840  bytes 7077746004 (6.5 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 432851  bytes 37838833 (36.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp7s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.242  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::9ada:bb2c:5175:e98  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:e4:b9:00  txqueuelen 1000  (Ethernet)
        RX packets 86550864  bytes 7291075951 (6.7 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 59045170  bytes 9724076359 (9.0 GiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp8s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.196.84.51  netmask 255.255.255.224  broadcast 10.196.84.63
        inet6 fd0d:deba:d97c:4b:c4e5:e4de:835c:35ee  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::ca98:3ace:3fb5:ccb3  prefixlen 64  scopeid 0x20<link>
        ether 52:54:00:db:14:ed  txqueuelen 1000  (Ethernet)
        RX packets 117706  bytes 8939582 (8.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2248  bytes 234948 (229.4 KiB)
```

31. Repeat steps 8 to 13 for IDIH Kafka and IDIH Service VMs.

32. Ensure that you are able to reach the IMI IPs of Mysql VM and Kafka VM from Service VM.

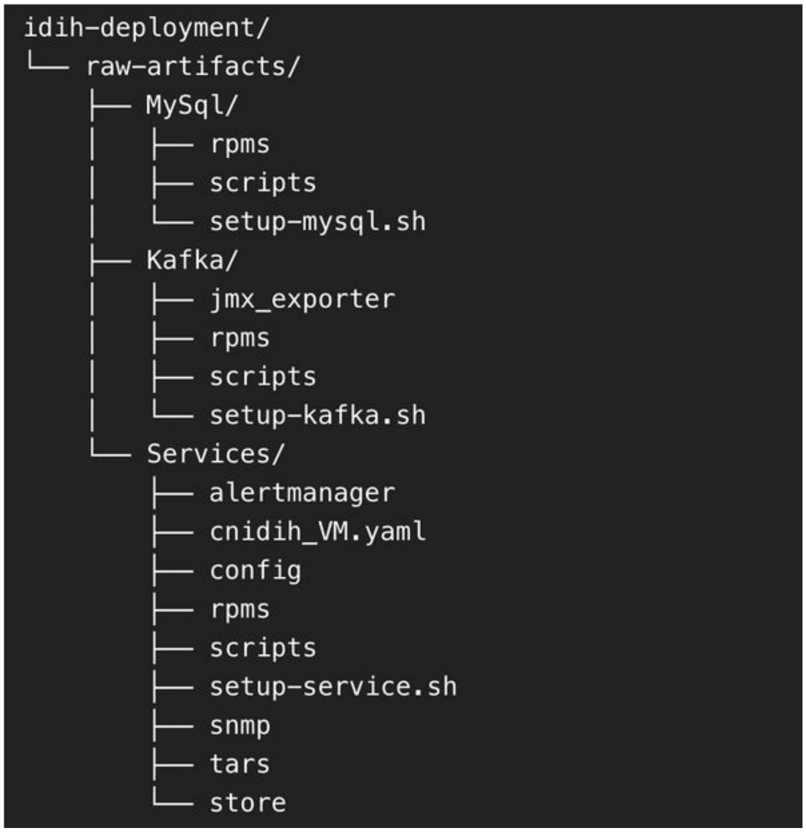
Installation Package Download and Extraction

The installation TAR file can be downloaded on any of the three VMs. After downloaded, extract (untar) the TAR file.

Directory Structure

After extraction, the directory structure will appear as follows:

Figure 5-21 Directory Structure



```
idih-deployment/
└── raw-artifacts/
    ├── MySql/
    │   ├── rpms
    │   ├── scripts
    │   └── setup-mysql.sh
    ├── Kafka/
    │   ├── jmx_exporter
    │   ├── rpms
    │   ├── scripts
    │   └── setup-kafka.sh
    └── Services/
        ├── alertmanager
        ├── cnidih_VM.yaml
        ├── config
        ├── rpms
        ├── scripts
        ├── setup-service.sh
        ├── snmp
        ├── tars
        └── store
```

Deployment of Components Across VMs

Distribute the extracted directories to their respective VMs as follows:

- Copy the MySql directory to the MySQL VM at any preferred location.
- Copy the Kafka directory to the Kafka VM at any preferred location.
- Copy the Services directory to the Services VM at any preferred location.

MySQL Setup

Perform the following steps to set up MySQL on the MySQL VM:

1. Access the MySQL VM:
   a. Log in and navigate to the MySQL directory.
   b. Run the MySQL Setup Script

i. Locate `setup-mysql.sh`.

ii. Run the below command to run the script:

```
./setup-mysql.sh
```

c. Configuration During Execution: Enter the IMI IP of the MySQL VM when prompted for the MySQL bind address.
Completion: After the script is complete, MySQL will be successfully set up on the VM.

Kafka Setup

Perform the following steps to set up Kafka on the Kafka VM:

1. Access the Kafka VM: Log in and navigate to the Kafka directory.
2. Run the Kafka Setup Script:
   a. Locate the setup-kafka.sh script
   b. Run the below command for the script:

   ```
   ./setup-kafka.sh
   ```

3. Configuration during execution:
   a. When prompted, enter the Kafka IMI IP and Kafka XSI IP. when prompted by the script.
   b. Kafka and Kraft services will be initiated on the specified IPs.

   After the successful health check is completed, Kafka will be successfully set up on VM.
4. Optional step, only if you need to use Kafka XMI IP instead of the default Kafka IMI IP for communication with DSR.
   a. Uncomment:

   ```
   advertised.listeners=INTERNAL_PLAINTEXT://
   192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093,EXTERNAL://
   [kafka_xmi]:9094 line in broker.properties file(path: /opt/kafka/
   config) and replace[kafka_xmi] with Kafka XMI IP
   ```

   b. Comment:

   ```
   advertised.listeners=INTERNAL_PLAINTEXT://
   192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093, EXTERNAL://
   10.196.84.46:9094 line.
   ```

   c. Run the below commands to restart Kraft and Kafka services:

   ```
   systemctl restart kafka
   ```

   After successful execution of the health check, Kafka is successfully set up on VM.

Service Setup

Perform the following steps to set up the services on the Service VM:

1. Access the Service VM
2. Navigate to the directory where the `setup-service.sh` script is located.

3. Move the store Directory to the `/opt/` path using the following command:

   ```
   mv store /opt/
   ```

4. Edit the Docker-compose file:
   a. Navigate to the `Services/ directory`.
   b. Edit `cnidih_VM.yaml` file:
      i. <REPLACE WITH SOAM VIP> must be replaced with a valid active SOAM IP.
      ii. Navigate to Protrace section and enable the following property `NFCONFIG_CLIENT_ENABLED` to **True**.
      iii. Save and exit.
   c. Run the following command for the Service Setup Script:

      ```
      ./setup-service.sh
      ```

5. Configuration during execution
   a. The script will prompt for several inputs during execution:
      i. Enter Service IMI IP, Service XMI IP, Kafka IMI IP, and MySQL IMI IP.

         > **Note**
         >
         > For IPv6 setups, the above IPs must be entered in square brackets ([]).

         After these inputs are provided, the script will start the required services and proceed with the health check.
      ii. Run the following command to verify if all services are running:

         ```
         podman ps -a
         ```

         Access the UI at: `https://<SERVICE XMI IP>/#/`

   Conclusion: This completes the setup for MySQL, Kafka, and Services. The deployment is now ready for use.

5.5.2 IDIH Raw Setup

Pre-installation Requirements for IDIH Deployment

Ensure that three separate virtual machines (VMs) are provisioned with OL8.9 dev ISO image and the appropriate resource allocation as specified in the Resource Requirements for IDIH:

1. Create three VMs:
   a. Click new VM
   b. Enter the following details:
      i. name
      ii. computer name
      iii. Type: New

iv. Guest OS family: Linux

v. Guest OS: Oracle Linux 8 (64 bit)

vi. Boot Image: OracleLinux-R8-U10-x86_64-dvd.iso

vii. Boot Firmware: BIOS

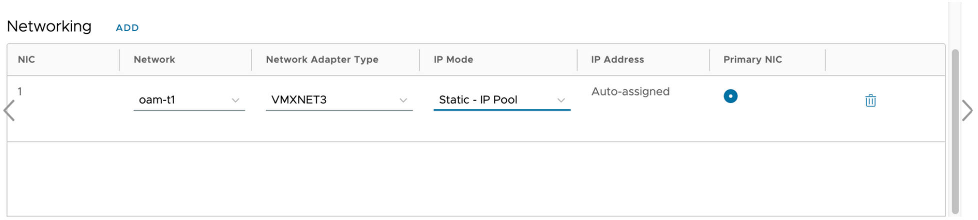
viii. For CPU, Memory, and Storage, refer to the IDIH Flavor Value table.

ix. Networking: (xmi, imi and xsi interface to be attached)
Refer the following table for flavors:

Table 5-12 IDIH Flavor Value

Flavor Name	VCPUs	RAM(GB)	Root Disk(GB)	Ephemeral	Swap Disk
kafka_flavor	6	16	170	0	0
Mysql-DB-DataNode	6	16	220	0	0
service_profile	6	16	120	0	0

Figure 5-22 Networking



Networking ADD

NIC	Network	Network Adapter Type	IP Mode	IP Address	Primary NIC
1	oam-t1	VMXNET3	Static - IP Pool	Auto-assigned	●

c. Launch and configure VMs:

i. Click Launch Web Console and install the OS.

ii. Configure networks in each VM and interface (xmi, imi, xsi):

```
nmcli device connect <interface-name>
nmcli connection modify ens256 +ipv4.address <ip-address>/
24nmcliconnection up <interface-name>
```

Ensure all necessary ports are accessible across XMI, XSI, and IMI interfaces on all three VMs.

Open ports on VMware:

```
[root@localhost ~]# firewall-cmd --add-port=9092/tcp --permanent
success
[root@localhost ~]# firewall-cmd --reload
success
[root@localhost ~]# firewall-cmd --list-ports
9092/tcp
```

2. Installation Package Download and Extraction:

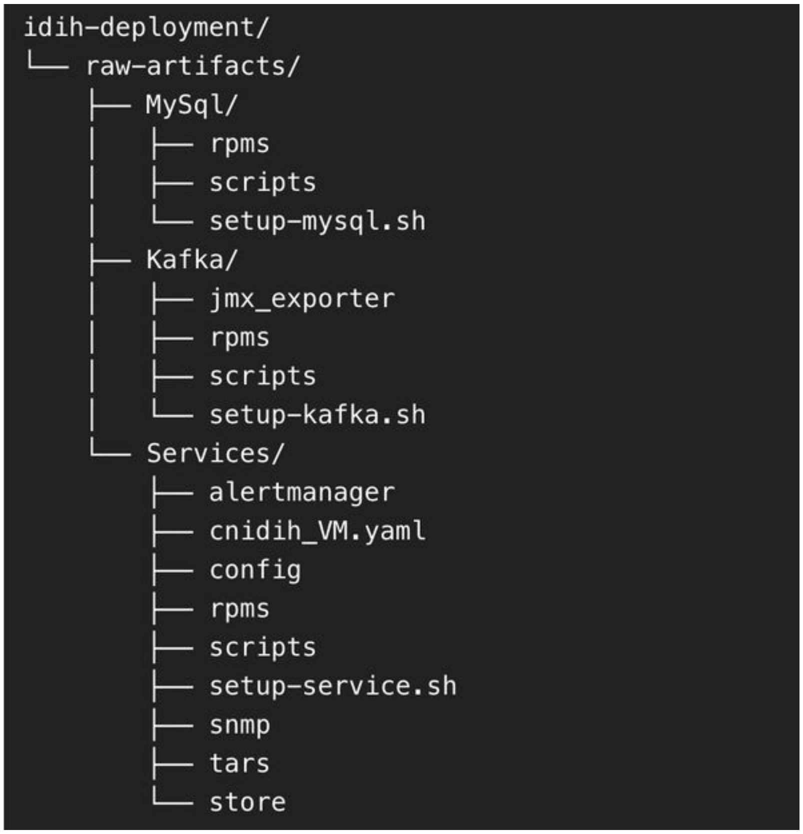
a. Download the installation TAR file on any of the three VMs.

b. Extract the TAR file:

```
tar -xvf <tar-file-name>.tar
```

3. Directory Structure: After extraction, the directory structure will be as follows:

Figure 5-23 Directory Structure



```
idih-deployment/
└── raw-artifacts/
    ├── MySql/
    │   ├── rpms
    │   ├── scripts
    │   └── setup-mysql.sh
    ├── Kafka/
    │   ├── jmx_exporter
    │   ├── rpms
    │   ├── scripts
    │   └── setup-kafka.sh
    └── Services/
        ├── alertmanager
        ├── cnidih_VM.yaml
        ├── config
        ├── rpms
        ├── scripts
        ├── setup-service.sh
        ├── snmp
        ├── tars
        └── store
```

4. Deployment of components across VMs:
   a. Distribute directories:
      i. MySQL directory to MySQL VM
      ii. Kafka directory to Kafka VM
      iii. Services directory to Service VM
5. MySQL Setup
   Perform the following procedure to set up MySQL on the MySQL VM:
   a. Access the MySQL VM:
      i. Log in and navigate to the MySQL directory.
      ii. Run the MySQL Setup Script:
         i. Locate `setup-mysql.sh`.
         ii. Run the below command to run the script:

```
./setup-mysql.sh
```

   iii. Configuration During Execution: Enter the IMI IP of the MySQL VM when prompted for the MySQL bind address.
   Completion: After the script is complete, MySQL will be successfully set up on the VM.

6. Kafka Setup
   a. Access the Kafka VM: Log in and navigate to the Kafka directory.
   b. Run the Kafka Setup Script:
      i. Locate the setup-kafka.sh script
      ii. Run the below command for the script:

```
./setup-kafka.sh
```

   c. Configuration during execution
      i. When prompted, enter the Kafka IMI IP and Kafka XSI IP. when prompted by the script.
      ii. Kafka and Kraft services will be initiated on the specified IPs.

   After the successful health check is completed, Kafka will be successfully set up on VM.

   d. Optional step, only if you need to use Kafka XMI IP instead of the default Kafka IMI IP for communication with DSR.
      i. Uncomment:

```
advertised.listeners=INTERNAL_PLAINTEXT://
192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093,EXTERNAL://
[kafka_xmi]:9094 line in broker.properties file(path: /opt/kafka/
config) and replace[kafka_xmi] with Kafka XMI IP
```

      ii. Comment:

```
advertised.listeners=INTERNAL_PLAINTEXT://
192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093, EXTERNAL://
10.196.84.46:9094 line.
```

      iii. Run the below commands to restart Kraft and Kafka services:

```
systemctl restart kafka
```

   After successful execution of the health check, Kafka is successfully set up on VM.

7. Service Setup
   a. Access the Service VM
   b. Navigate to the directory where the `setup-service.sh` script is located.
   c. Move the store Directory to the `/opt/` path using the following command:

```
mv store /opt/
```

   d. Edit the Docker-compose file:
      i. Navigate to the `Services/ directory`.

ii. Edit `cnidih_VM.yaml` file:

   i. <REPLACE WITH SOAM VIP> must be replaced with a valid active SOAM IP.

   ii. Navigate to Protrace section and enable the following property `NFCONFIG_CLIENT_ENABLED` to true.

   iii. Save and exit.

iii. Run the following command for the Service Setup Script:

```
./setup-service.sh
```

e. Configuration during execution: The script will prompt for several inputs during execution:

   i. Enter Service IMI IP, Service XMI IP, Kafka IMI IP, and MySQL IMI IP.

   > **Note**
   >
   > For IPv6 setups, the above IPs must be entered in square brackets ([]).

   After these inputs are provided, the script will start the required services and proceed with the health check.

   ii. Run the following command to verify if all services are running:

```
podman ps -a
```

   Access the UI at: `https://<SERVICE XMI IP>/#/`

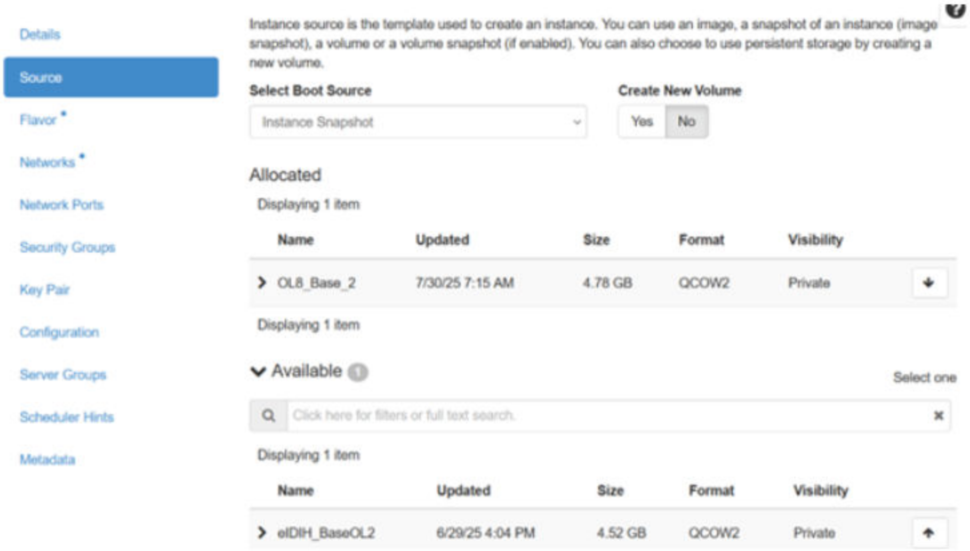
Conclusion: This completes the setup for MySQL, Kafka, and Services. The deployment is now ready for use.

5.5.3 IDIH Deployment on OpenStack with RAW Images

Perform the following procedure for IDIH Deployment on OpenStack with RAW Images:

1. Login to OpenStack with valid credentials.
2. Ensure appropriate flavors are available before launching instances.
3. Launch MySQL VM:
   a. Navigate to **Compute**, **Instances** and click **Launch Instance**.
   b. Provide an instance name, example: mysql-openstack
   c. Select the image (preferably ol8.10) and ensure **Create New Volume** is set to **NO**.

Figure 5-24 Source



Instance source is the template used to create an instance. You can use an image, a snapshot of an instance (image snapshot), a volume or a volume snapshot (if enabled). You can also choose to use persistent storage by creating a new volume.

Select Boot Source: Instance Snapshot

Create New Volume: Yes [✓ No]

Allocated

Displaying 1 item

Name	Updated	Size	Format	Visibility
OL8_Base_2	7/30/25 7:15 AM	4.78 GB	QCOW2	Private

Displaying 1 item

Available 1 — Select one

Click here for filters or full text search.

Displaying 1 item

Name	Updated	Size	Format	Visibility
eIDIH_BaseOL2	6/29/25 4:04 PM	4.52 GB	QCOW2	Private

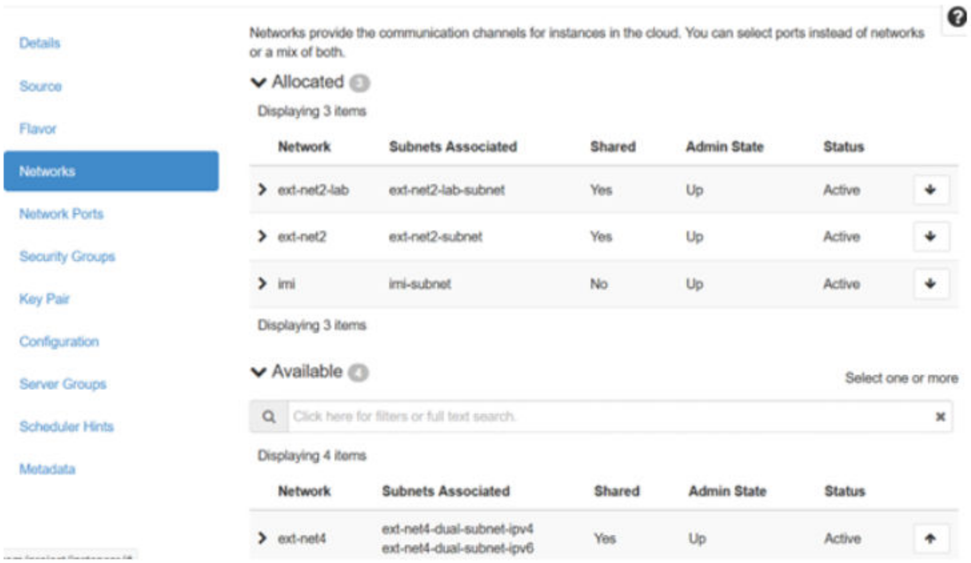
d. Select the appropriate flavor for the MySQL VM as specified in the following table.

Table 5-13 IDIH Flavor Value

Flavor Name	VCPUs	RAM(GB)	Root Disk(GB)	Ephemeral	Swap Disk
kafka_flavor	6	16	170	0	0
Mysql-DB-DataNode	6	16	220	0	0
service_profile	6	16	120	0	0

e. Add XMI, IMI, and XSI networks to the VM.

Figure 5-25 Networks



Networks provide the communication channels for instances in the cloud. You can select ports instead of networks or a mix of both.

Allocated 3

Displaying 3 items

Network	Subnets Associated	Shared	Admin State	Status
ext-net2-lab	ext-net2-lab-subnet	Yes	Up	Active
ext-net2	ext-net2-subnet	Yes	Up	Active
imi	imi-subnet	No	Up	Active

Displaying 3 items

Available 4 — Select one or more

Click here for filters or full text search.

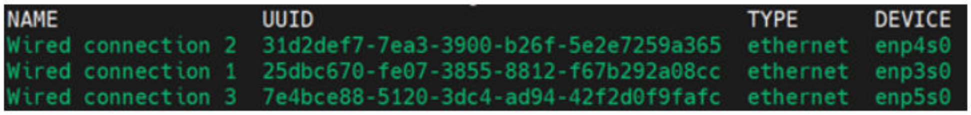
Displaying 4 items

Network	Subnets Associated	Shared	Admin State	Status
ext-net4	ext-net4-dual-subnet-ipv4 ext-net4-dual-subnet-ipv6	Yes	Up	Active

   f. Click **Launch Instance** to create the MySQL VM.

4. Configure Network Interfaces:
   a. Once the VM is created, access the console and log in with `root/changeme` credentials.
   b. Run nmcli con show to list network interfaces.

Figure 5-26 Command



```
NAME                 UUID                                  TYPE      DEVICE
Wired connection 2   31d2def7-7ea3-3900-b26f-5e2e7259a365  ethernet  enp4s0
Wired connection 1   25dbc670-fe07-3855-8812-f67b292a08cc  ethernet  enp3s0
Wired connection 3   7e4bce88-5120-3dc4-ad94-42f2d0f9fafc  ethernet  enp5s0
```

5. **Disable IPv6 and configure IPv4 for the XMI interface (Optional step):**
   a. nmcli con mod <xmi_interface_name> ipv6.method disabled
   b. nmcli con mod <xmi_interface_name> ipv4.address <xmi_ip_address/cidr> ipv4.gateway <xmi_gateway> ipv4.route-metric 1 ipv4.method manual
   c. nmcli con up <xmi_interface_name>
      SSH to the MySQL VM using the XMI IP and configure IMI and XSI interfaces similarly.
   d. Repeat for Kafka and Service VMs: Perform steps 1 to 12 for Kafka and Service VMs (**Mandatory step**).

6. Verify Connectivity:
   a. Ensure all VMs can reach each other using their IMI IPs:
      i. On all VMs, check firewall status:

```
sudo systemctl status firewalld
```

      ii. If not running, start and enable it:

```
sudo systemctl start firewalld
        sudo systemctl enable firewalld
```

      iii. Edit `/etc/resolv.conf` to include:

```
# Generated by NetworkManager
        search openstack.internal novalocal
        nameserver <nameserver_ip
```

      iv. Edit `/etc/dnf/dnf.conf` to ensure no ash proxy is present:

```
[main]
gpgcheck=1
installonly_limit=3
clean_requirements_on_remove=True
best=True
proxy=http://www-proxy.us.oracle.com:80
retries=100
```

v. Clean DNF cache:

```
sudo dnf clean all
```

vi. Install utilities:

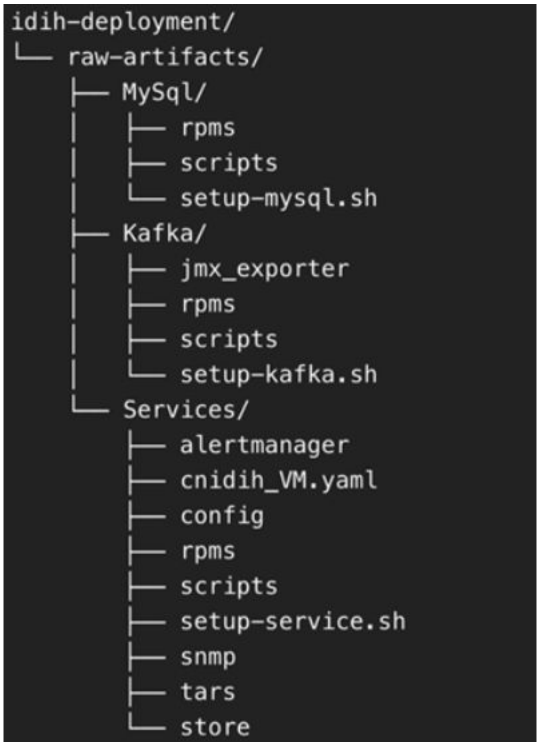
```
sudo dnf install tar dos2unix
```

7. Installation and Extraction:

   a. Download and extract the installation TAR file on any VM.

   b. Directory structure post extraction:

Figure 5-27 Directory Structure post Extraction



```
idih-deployment/
└── raw-artifacts/
    ├── MySql/
    │   ├── rpms
    │   ├── scripts
    │   └── setup-mysql.sh
    ├── Kafka/
    │   ├── jmx_exporter
    │   ├── rpms
    │   ├── scripts
    │   └── setup-kafka.sh
    └── Services/
        ├── alertmanager
        ├── cnidih_VM.yaml
        ├── config
        ├── rpms
        ├── scripts
        ├── setup-service.sh
        ├── snmp
        ├── tars
        └── store
```

   c. Distribute directories:

      i. MySQL directory to MySQL VM

      ii. Kafka directory to Kafka VM

      iii. Services directory to Service VM

8. MySQL Setup

   a. Access the MySQL VM:

      i. Log in and navigate to the MySQL directory.

      ii. Run the MySQL Setup Script

         i. Locate `setup-mysql.sh`.

         ii. Run the below command to run the script:

```
./setup-mysql.sh
```

iii. Configuration During Execution: Enter the IMI IP of the MySQL VM when prompted for the MySQL bind address.
Completion: After the script is complete, MySQL will be successfully set up on the VM.

9. Kafka Setup

   a. Access the Kafka VM: Log in and navigate to the Kafka directory.

   b. Run the Kafka Setup Script

      i. Locate the setup-kafka.sh script

      ii. Run the below command for the script:

```
./setup-kafka.sh
```

   c. Configuration during execution

      i. When prompted, enter the Kafka IMI IP and Kafka XSI IP. when prompted by the script.

      ii. Kafka and Kraft services will be initiated on the specified IPs.

   d. Optional step, only if you need to use Kafka XMI IP instead of the default Kafka IMI IP for communication with DSR.

      i. Uncomment:

```
advertised.listeners=INTERNAL_PLAINTEXT://
192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093,EXTERNAL://
[kafka_xmi]:9094 line in broker.properties file(path: /opt/kafka/
config) and replace[kafka_xmi] with Kafka XMI IP
```

      ii. Comment:

```
advertised.listeners=INTERNAL_PLAINTEXT://
192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093, EXTERNAL://
10.196.84.46:9094 line.
```

      iii. Run the below command to restart Kraft and Kafka services:

```
systemctl restart kafka
```

   After successful execution of the health check, Kafka is successfully set up on VM.

10. Service Setup

   a. Access the Service VM

   b. Navigate to the directory where the `setup-service.sh` script is located.

   c. Move the store Directory to the `/opt/` path using the following command:

```
mv store /opt/
```

   d. Edit the Docker-compose file:

      i. Navigate to the `Services/ directory`.

      ii. Edit `cnidih_VM.yaml` file:

         i. <REPLACE WITH SOAM VIP> must be replaced with a valid active SOAM IP.

ii. Navigate to Protrace section and enable the following property: `NFCONFIG_CLIENT_ENABLED` to **True**.

iii. Save and exit.

iii. Run the following command for the Service Setup Script:

```
./setup-service.sh
```

e. Configuration during execution: The script will prompt for several inputs during execution:

i. Enter Service IMI IP, Service XMI IP, Kafka IMI IP, and MySQL IMI IP.

> **Note**
>
> For IPv6 setups, the above IPs must be entered in square brackets ([]).

After these inputs are provided, the script will start the required services and proceed with the health check.

ii. Run the following command to verify if all services are running:

```
podman ps -a
```

Access the UI at: `https://<SERVICE XMI IP>/#/`

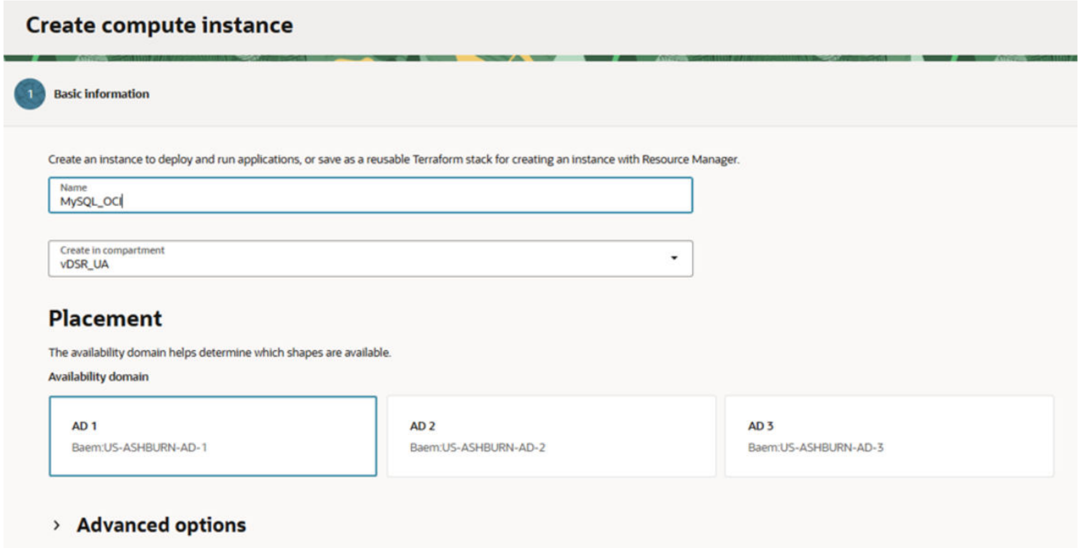
This completes the setup for MySQL, Kafka, and Services. The deployment is now ready for use.

5.5.4 IDIH Deployment on Oracle Cloud Infrastructure (OCI) with RAW Images

Perform the following procedure for IDIH Deployment on OCI with RAW Images:

1. Login to OCI with valid credentials.
2. Navigate to **Compute**, **Instances**, and click **Create Instance**.
3. Provide an instance name for MySQL VM. Example: MySQL_OCI.

Figure 5-28   Create Compute instance



Create compute instance

1 Basic information

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name: MySQL_OCI

Create in compartment: vDSR_UA

Placement

The availability domain helps determine which shapes are available.

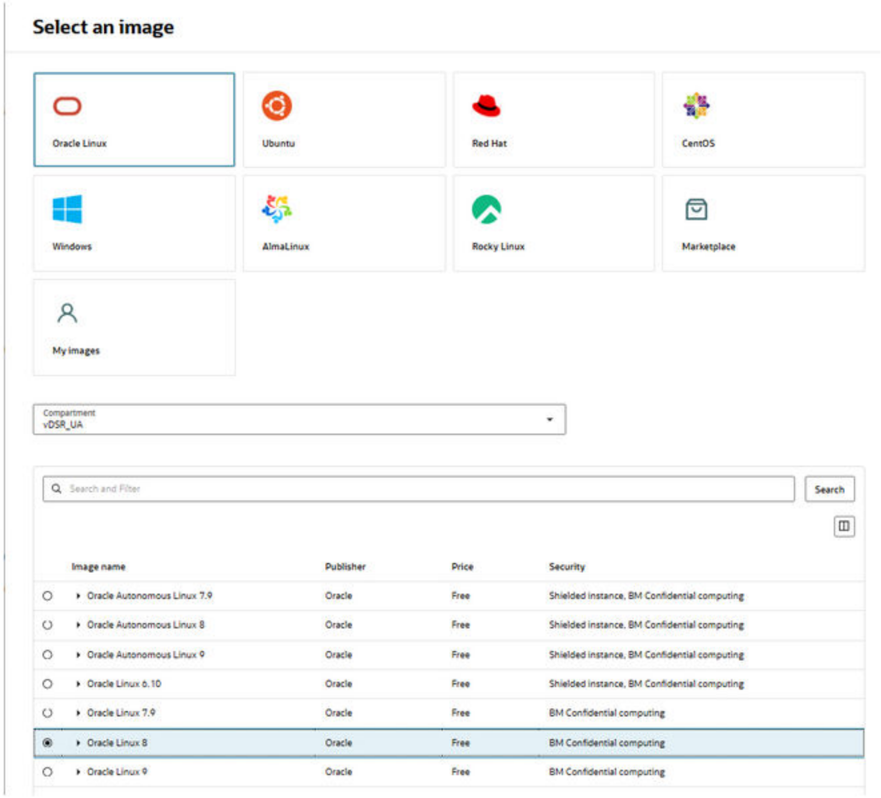
Availability domain

AD 1	AD 2	AD 3
Baem:US-ASHBURN-AD-1	Baem:US-ASHBURN-AD-2	Baem:US-ASHBURN-AD-3

› Advanced options

4. Click **Change Image**, select **Oracle Linux 8**, and click **Select Image**.

Figure 5-29   Select an Image



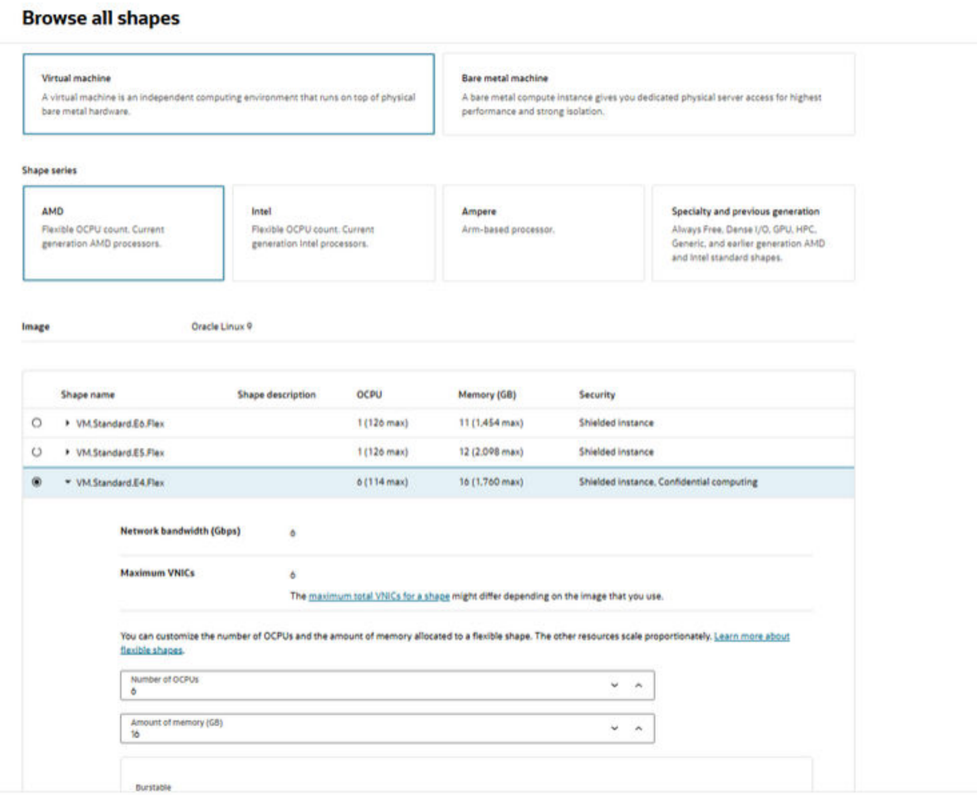
Select an image

Compartment: vDSR_UA

	Image name	Publisher	Price	Security
○	▸ Oracle Autonomous Linux 7.9	Oracle	Free	Shielded instance, BM Confidential computing
○	▸ Oracle Autonomous Linux 8	Oracle	Free	Shielded instance, BM Confidential computing
○	▸ Oracle Autonomous Linux 9	Oracle	Free	Shielded instance, BM Confidential computing
○	▸ Oracle Linux 6.10	Oracle	Free	Shielded instance, BM Confidential computing
○	▸ Oracle Linux 7.9	Oracle	Free	BM Confidential computing
●	▸ Oracle Linux 8	Oracle	Free	BM Confidential computing
○	▸ Oracle Linux 9	Oracle	Free	BM Confidential computing

5. Click **Change Shape**, select an appropriate shape based on the requirements and availability in the OCI compartment. Adjust the number of OCPU such as the number of vCPUs remains 6. Memory size is 16 GB. Click **Select Shape** and click **Next**.

Figure 5-30 Browse all Shapes



Browse all shapes

Virtual machine
A virtual machine is an independent computing environment that runs on top of physical bare metal hardware.

Bare metal machine
A bare metal compute instance gives you dedicated physical server access for highest performance and strong isolation.

Shape series

AMD
Flexible OCPU count. Current generation AMD processors.

Intel
Flexible OCPU count. Current generation Intel processors.

Ampere
Arm-based processor.

Specialty and previous generation
Always Free, Dense I/O, GPU, HPC, Generic, and earlier generation AMD and Intel standard shapes.

Image: Oracle Linux 9

	Shape name	Shape description	OCPU	Memory (GB)	Security
○	▸ VM.Standard.E6.Flex		1 (126 max)	11 (1,454 max)	Shielded instance
○	▸ VM.Standard.E5.Flex		1 (126 max)	12 (2,098 max)	Shielded instance
●	▾ VM.Standard.E4.Flex		6 (114 max)	16 (1,760 max)	Shielded instance, Confidential computing

Network bandwidth (Gbps): 6

Maximum VNICs: 6
The maximum total VNICs for a shape might differ depending on the image that you use.

You can customize the number of OCPUs and the amount of memory allocated to a flexible shape. The other resources scale proportionately. Learn more about flexible shapes.

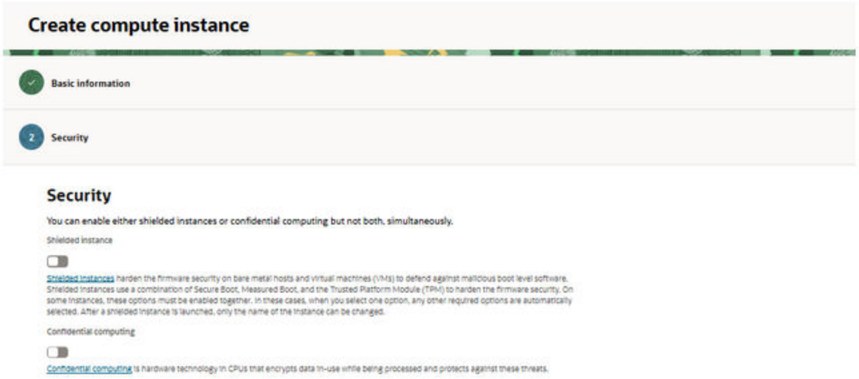
Number of OCPUs: 6

Amount of memory (GB): 16

Burstable

6. No changes are required in **Security**. Click **Next**.

Figure 5-31 Create Compute Instance



Create compute instance

✓ Basic information

2 Security

Security

You can enable either shielded instances or confidential computing but not both, simultaneously.

Shielded instance

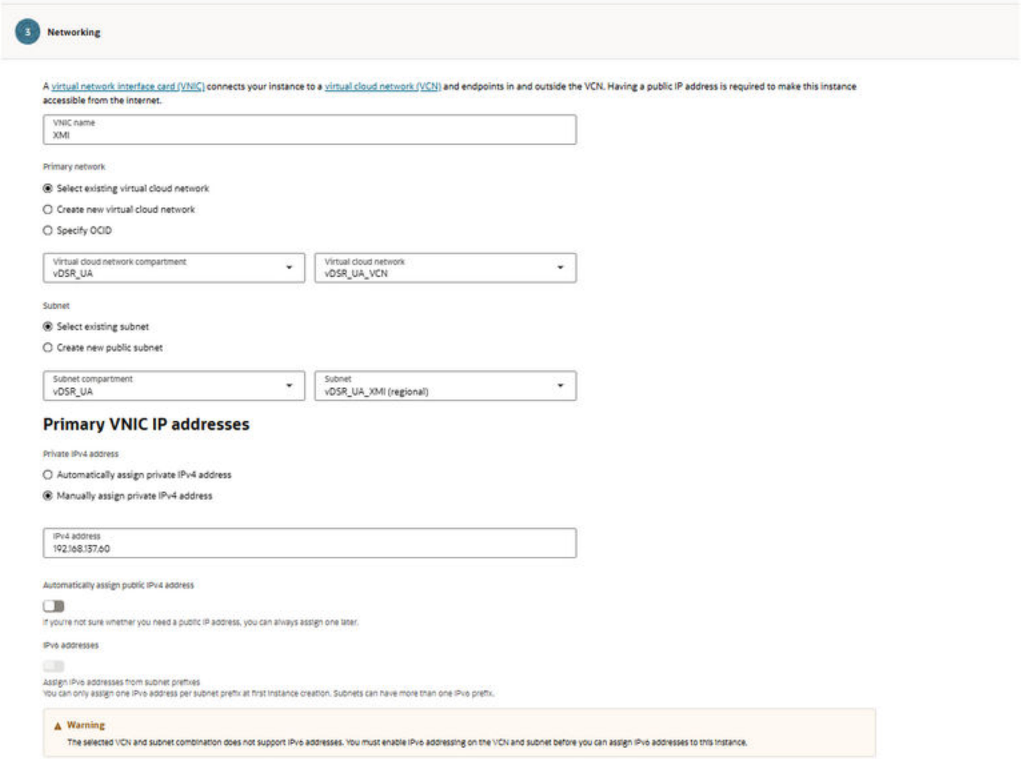
Shielded instances harden the firmware security on bare metal hosts and virtual machines (VMs) to defend against malicious boot level software. Shielded instances use a combination of Secure Boot, Measured Boot, and the Trusted Platform Module (TPM) to harden the firmware security. On some instances, these options must be enabled together. In these cases, when you select one option, any other required options are automatically selected. After a shielded instance is launched, only the name of the instance can be changed.

Confidential computing

Confidential computing is hardware technology in CPUs that encrypts data in-use while being processed and protects against these threats.

7. In the **Networking**, define the XMI VNIC name, VCN, and XMI subnet. Manually assign an IPv4 address.

Figure 5-32 Networking



3 Networking

A virtual network interface card (VNIC) connects your instance to a virtual cloud network (VCN) and endpoints in and outside the VCN. Having a public IP address is required to make this instance accessible from the internet.

VNIC name: XMI

Primary network

● Select existing virtual cloud network
○ Create new virtual cloud network
○ Specify OCID

Virtual cloud network compartment: vDSR_UA
Virtual cloud network: vDSR_UA_VCN

Subnet

● Select existing subnet
○ Create new public subnet

Subnet compartment: vDSR_UA
Subnet: vDSR_UA_XMI (regional)

Primary VNIC IP addresses

Private IPv4 address

○ Automatically assign private IPv4 address
● Manually assign private IPv4 address

IPv4 address: 192.168.137.60

Automatically assign public IPv4 address

If you're not sure whether you need a public IP address, you can always assign one later.

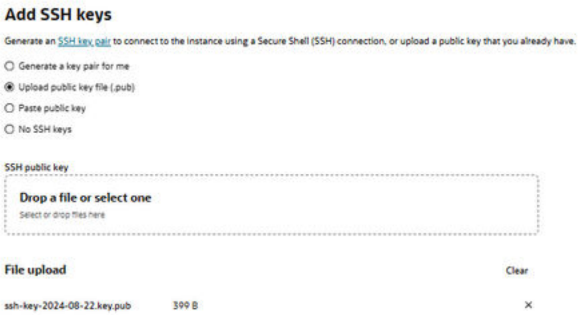
IPv6 addresses

Assign IPv6 addresses from subnet prefixes
You can only assign one IPv6 address per subnet prefix at first instance creation. Subnets can have more than one IPv6 prefix.

Warning
The selected VCN and subnet combination does not support IPv6 addresses. You must enable IPv6 addressing on the VCN and subnet before you can assign IPv6 addresses to this instance.

8. In **Add SSH keys**, select own key or generate a new one. Click **Next**.

Figure 5-33 SSH Keys



Add SSH keys

Generate an SSH key pair to connect to the instance using a Secure Shell (SSH) connection, or upload a public key that you already have.

○ Generate a key pair for me
● Upload public key file (.pub)
○ Paste public key
○ No SSH keys

SSH public key

Drop a file or select one
Select or drop files here

File upload Clear

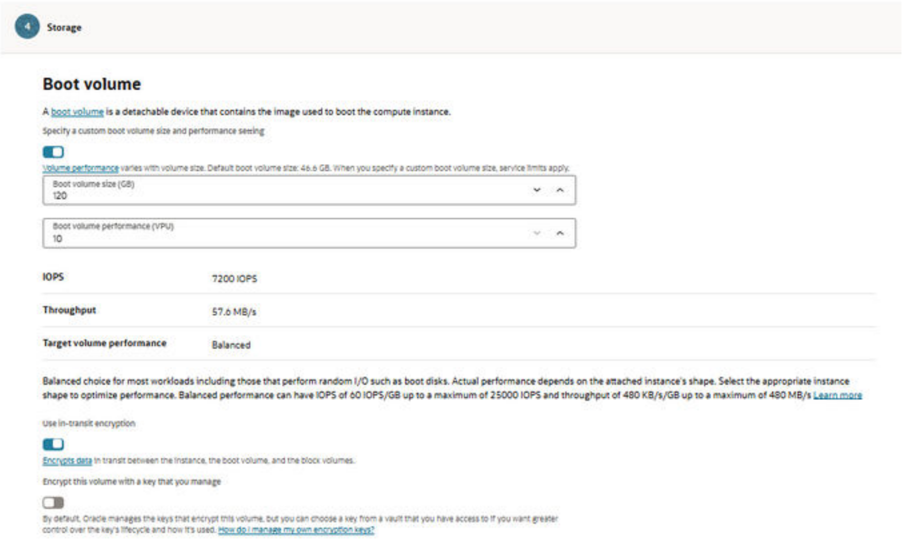
ssh-key-2024-08-22.key.pub 399 B ×

9. In the **Storage** section, specify a custom boot volume size for the VM and click **Next**.

Table 5-14 VM values

VM	Boot Volume Size GB
MySQL	220
Kafka	170 GB
Services	120

Figure 5-34 Boot Volume



Boot volume

A boot volume is a detachable device that contains the image used to boot the compute instance.

Specify a custom boot volume size and performance setting

Volume performance varies with volume size. Default boot volume size: 46.6 GB. When you specify a custom boot volume size, service limits apply.

Boot volume size (GB): 120

Boot volume performance (VPU): 10

IOPS	7200 IOPS
Throughput	57.6 MB/s
Target volume performance	Balanced

Balanced choice for most workloads including those that perform random I/O such as boot disks. Actual performance depends on the attached instance's shape. Select the appropriate instance shape to optimize performance. Balanced performance can have IOPS of 60 IOPS/GB up to a maximum of 25000 IOPS and throughput of 480 KB/s/GB up to a maximum of 480 MB/s Learn more

Use in-transit encryption

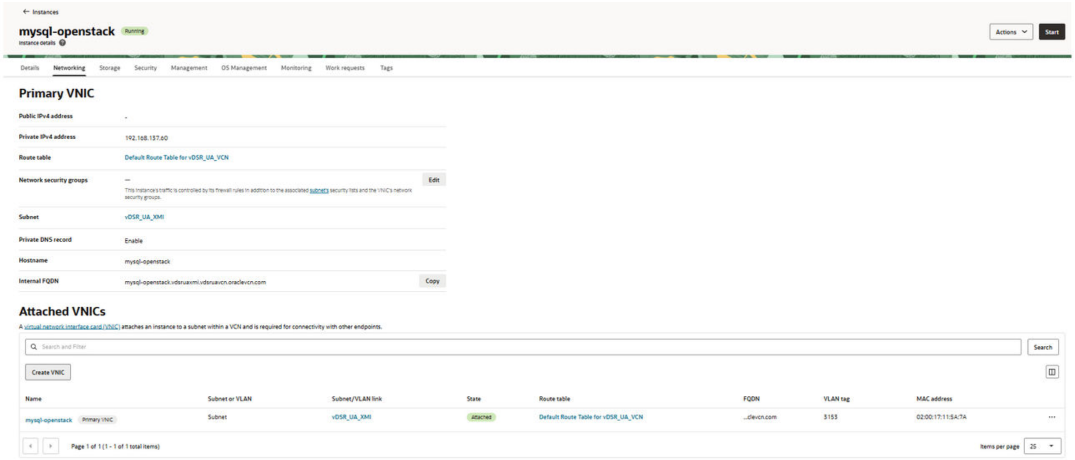
Encrypts data in transit between the instance, the boot volume, and the block volumes.

Encrypt this volume with a key that you manage

By default, Oracle manages the keys that encrypt this volume, but you can choose a key from a vault that you have access to if you want greater control over the key's lifecycle and how it's used. How do I manage my own encryption keys?

10. Review the configuration, if correct, click **Create**.
11. After the VM is created and running, navigate to **Networking** and click **Create VNIC**.

Figure 5-35 mysql-OpenStack



mysql-openstack

Primary VNIC

Public IPv4 address	-
Private IPv4 address	192.168.137.60
Route table	Default Route Table for vDSR_UA_VCN
Network security groups	— This instance's traffic is controlled by its firewall rules in addition to the associated subnet's security lists and the VNIC's network security groups.
Subnet	vDSR_UA_XMI
Private DNS record	Enable
Hostname	mysql-openstack
Internal FQDN	mysql-openstack.vdsruaxmi.vdsruavcn.oraclevcn.com

Attached VNICs

A virtual network interface card (VNIC) attaches an instance to a subnet within a VCN and is required for connectivity with other endpoints.

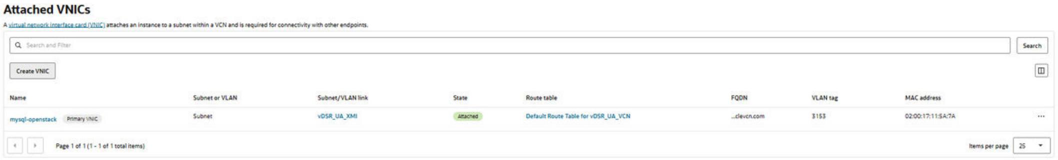
Name	Subnet or VLAN	Subnet/VLAN link	State	Route table	FQDN	VLAN tag	MAC address
mysql-openstack Primary VNIC	Subnet	vDSR_UA_XMI	Attached	Default Route Table for vDSR_UA_VCN	...clevcn.com	3153	02:00:17:11:5A:7A

Page 1 of 1 (1 - 1 of 1 total items)

Items per page 25

12. Provide a name for the IMI VNIC, select the IMI subnet, manually assign an IP, and click **Submit**, repeat step 10 for XSI1 VNIC.

Figure 5-36 Attached VNICs



Attached VNICs

A virtual network interface card (VNIC) attaches an instance to a subnet within a VCN and is required for connectivity with other endpoints.

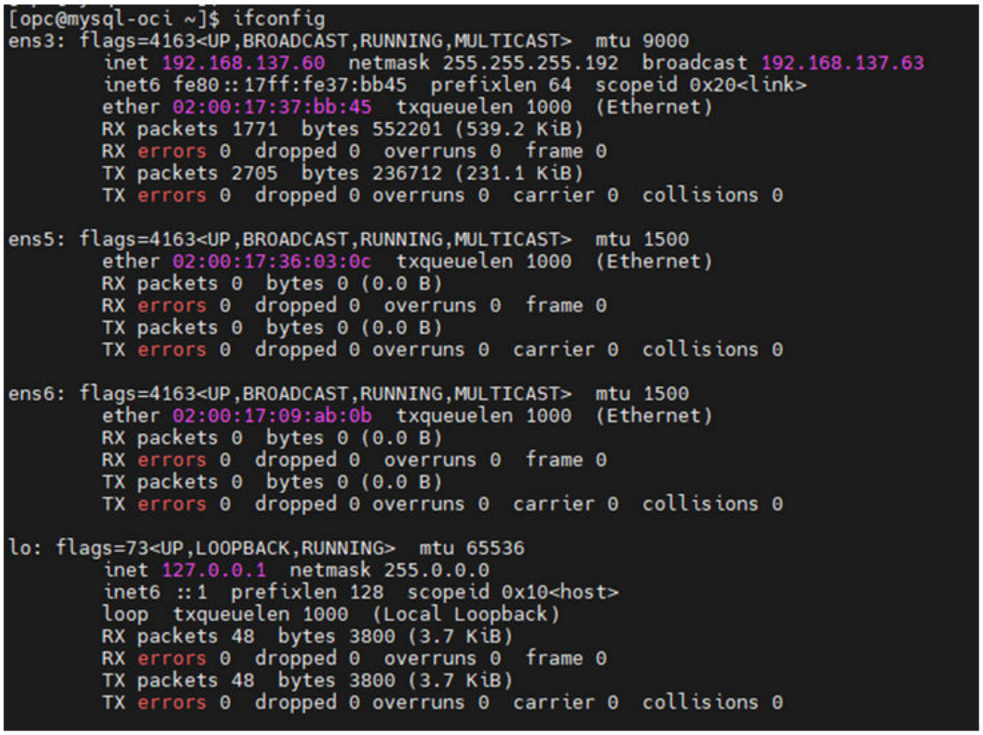
Name	Subnet or VLAN	Subnet/VLAN link	State	Route table	FQDN	VLAN tag	MAC address
mysql-openstack Primary VNIC	Subnet	vDSR_UA_XMI	Attached	Default Route Table for vDSR_UA_VCN	...clevcn.com	3153	02:00:17:11:5A:7A

Page 1 of 1 (1 - 1 of 1 total items)

Items per page 25

13. SSH into the MySQL VM using the XMI interface. Use the assigned IP and SSH key. The only interface with an IP assigned is **ens3**.

Figure 5-37 ifconfig



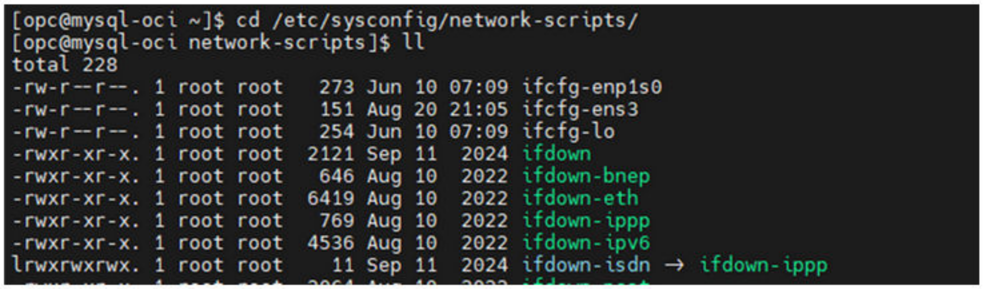
```
[opc@mysql-oci ~]$ ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9000
        inet 192.168.137.60  netmask 255.255.255.192  broadcast 192.168.137.63
        inet6 fe80::17ff:fe37:bb45  prefixlen 64  scopeid 0x20<link>
        ether 02:00:17:37:bb:45  txqueuelen 1000  (Ethernet)
        RX packets 1771  bytes 552201 (539.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2705  bytes 236712 (231.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 02:00:17:36:03:0c  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 02:00:17:09:ab:0b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 48  bytes 3800 (3.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 48  bytes 3800 (3.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

14. Network scripts

    a. Configure ens5 and ens6 by navigating to:

    ```
    "cd /etc/sysconfig/network-scripts/"and"ll"
    ```

    Figure 5-38 Network Scripts

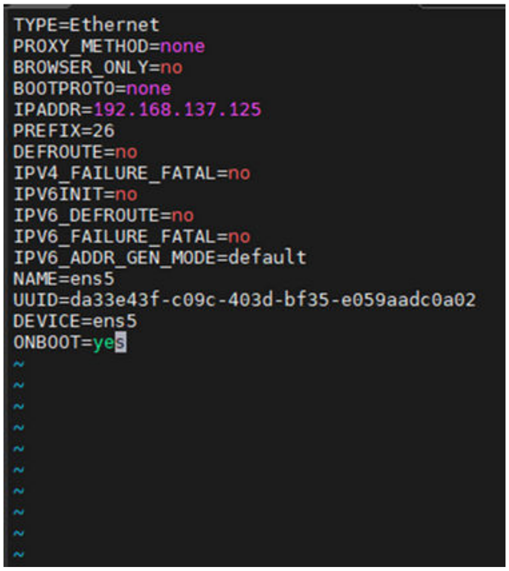
    

    ```
    [opc@mysql-oci ~]$ cd /etc/sysconfig/network-scripts/
    [opc@mysql-oci network-scripts]$ ll
    total 228
    -rw-r--r--. 1 root root  273 Jun 10 07:09 ifcfg-enp1s0
    -rw-r--r--. 1 root root  151 Aug 20 21:05 ifcfg-ens3
    -rw-r--r--. 1 root root  254 Jun 10 07:09 ifcfg-lo
    -rwxr-xr-x. 1 root root 2121 Sep 11  2024 ifdown
    -rwxr-xr-x. 1 root root  646 Aug 10  2022 ifdown-bnep
    -rwxr-xr-x. 1 root root 6419 Aug 10  2022 ifdown-eth
    -rwxr-xr-x. 1 root root  769 Aug 10  2022 ifdown-ippp
    -rwxr-xr-x. 1 root root 4536 Aug 10  2022 ifdown-ipv6
    lrwxrwxrwx. 1 root root   11 Sep 11  2024 ifdown-isdn -> ifdown-ippp
    ```

    b. Run the following commands as **root** to configure the interfaces:

    c. Configure the IMI interface:

Figure 5-39   Ethernet

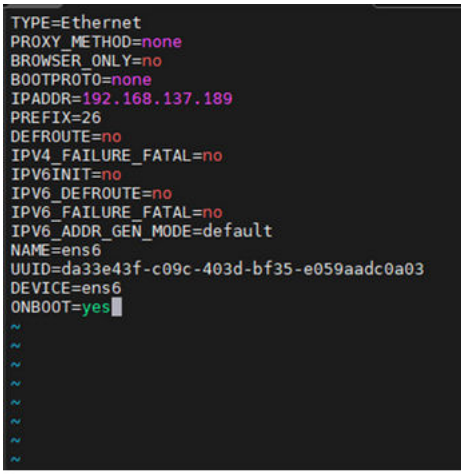


```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=192.168.137.125
PREFIX=26
DEFROUTE=no
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_DEFROUTE=no
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=default
NAME=ens5
UUID=da33e43f-c09c-403d-bf35-e059aadc0a02
DEVICE=ens5
ONBOOT=yes
~
~
~
~
~
~
~
~
~
~
```

d. Save and close.

e. Configure the XSI1 interface

Figure 5-40   XSI Interface



```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=192.168.137.189
PREFIX=26
DEFROUTE=no
IPV4_FAILURE_FATAL=no
IPV6INIT=no
IPV6_DEFROUTE=no
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=default
NAME=ens6
UUID=da33e43f-c09c-403d-bf35-e059aadc0a03
DEVICE=ens6
ONBOOT=yes
~
~
~
~
~
~
~
~
```

f. Run the following command to restart the VM:

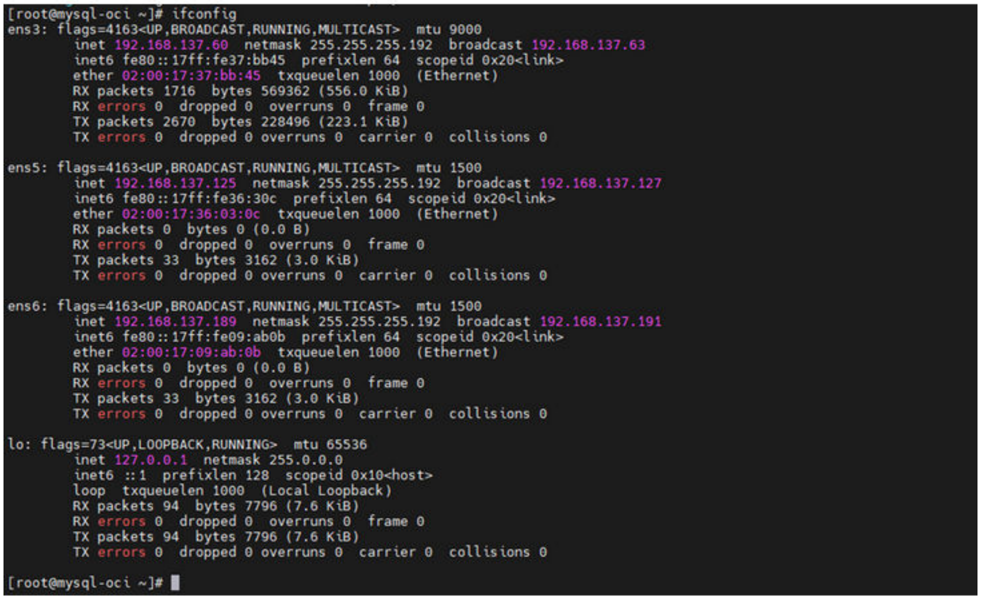
```
[]# sudo init 6
```

g. Verify Network Interfaces: After the restart, verify if ens3, ens5, and ens6 interfaces consist IP address by running the following command:

```
[]# ifconfig
```

Ensure the interfaces are up and running. Perform steps 1 to 22 for Kafka and Service VMs as well.

Figure 5-41   ifconfig



```
[root@mysql-oci ~]# ifconfig
ens3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9000
        inet 192.168.137.60  netmask 255.255.255.192  broadcast 192.168.137.63
        inet6 fe80::17ff:fe37:bb45  prefixlen 64  scopeid 0x20<link>
        ether 02:00:17:37:bb:45  txqueuelen 1000  (Ethernet)
        RX packets 1716  bytes 569362 (556.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2670  bytes 228496 (223.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens5: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.137.125  netmask 255.255.255.192  broadcast 192.168.137.127
        inet6 fe80::17ff:fe36:30c  prefixlen 64  scopeid 0x20<link>
        ether 02:00:17:36:03:0c  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 3162 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens6: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.137.189  netmask 255.255.255.192  broadcast 192.168.137.191
        inet6 fe80::17ff:fe09:ab0b  prefixlen 64  scopeid 0x20<link>
        ether 02:00:17:09:ab:0b  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 33  bytes 3162 (3.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 94  bytes 7796 (7.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94  bytes 7796 (7.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[root@mysql-oci ~]# █
```

15. After creating 3 VMs, ensure you can reach between all 3 VMs using their IMI IPs.

16. Firewall Configuration (All 3 VMs):

    a. Run the following command to check firewall status:

    ```
    sudo systemctl status firewalld
    ```

    > **Note**
    >
    > Firewall must be disabled in Services VM.

    b. Run the following command if the firewall is not running, start and enable it:

    ```
    sudo systemctl start firewalld
    sudo systemctl enable firewalld
    ```

    c. Verify the firewall is running:

    ```
    sudo systemctl status firewalld
    ```

    d. DNS configuration

        i. Ensure the file `/etc/resolv.conf` file consists the required DNS configuration.

        ii. Verify that the **ash proxy** `proxy=http://www-proxy-ash7.us.oracle.com:80`is not present. Use the following configuration:

        ```
        [main]
        gpgcheck=1
        installonly_limit=3
        clean_requirements_on_remove=True
        ```

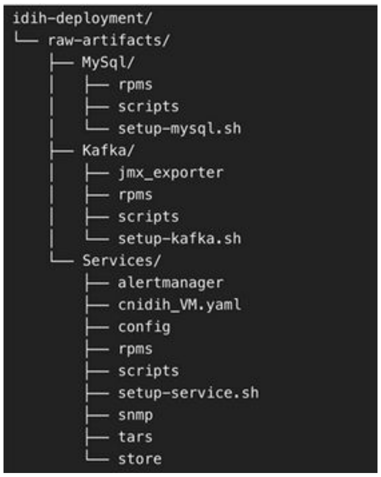
```
best=True
proxy=http://www-proxy.us.oracle.com:80
retries=100
```

iii. Unset proxies and run below commands to install tar and dos2unix utilities:

```
sudo dnf install tar
sudo dnf install dos2unix
```

17. Installation Package Download and Extraction: The installation TAR file can be downloaded on any of the three VMs. Extract (untar) the TAR file once downloaded.
18. Directory Structure: After extraction, the directory structure will appear as follows:

Figure 5-42 Directory Structure



```
idih-deployment/
└── raw-artifacts/
    ├── MySql/
    │   ├── rpms
    │   ├── scripts
    │   └── setup-mysql.sh
    ├── Kafka/
    │   ├── jmx_exporter
    │   ├── rpms
    │   ├── scripts
    │   └── setup-kafka.sh
    └── Services/
        ├── alertmanager
        ├── cnidih_VM.yaml
        ├── config
        ├── rpms
        ├── scripts
        ├── setup-service.sh
        ├── snmp
        ├── tars
        └── store
```

19. Deployment of Components Across VMs
    a. Distribute the extracted directories to their respective VMs:
        i. Copy the MySql directory to the MySQL VM at any preferred location.
        ii. Copy the Kafka directory to the Kafka VM at any preferred location.
        iii. Copy the Services directory to the Services VM at any preferred location.
20. MySQL Setup
    a. Access the MySQL VM:
        i. Log in and navigate to the MySQL directory.
        ii. Run the MySQL Setup Script
            i. Locate `setup-mysql.sh`.
            ii. Run the below command to run the script:

```
./setup-mysql.sh
```

        iii. Configuration During Execution: Enter the IMI IP of the MySQL VM when prompted for the MySQL bind address.
        Completion: After the script is complete, MySQL will be successfully set up on the VM.

21. Kafka Setup
    a. Access the Kafka VM: Log in and navigate to the Kafka directory.
    b. Run the Kafka Setup Script
        i. Locate the setup-kafka.sh script
        ii. Run the below command for the script:

        ```
        ./setup-kafka.sh
        ```

    c. Configuration during execution
        i. When prompted, enter the Kafka IMI IP and Kafka XSI IP. when prompted by the script.
        ii. Kafka and Kraft services will be initiated on the specified IPs.

        After the successful health check is completed, Kafka will be successfully set up on VM.

    d. Optional step, only if you need to use Kafka XMI IP instead of the default Kafka IMI IP for communication with DSR.
        i. Uncomment:

        ```
        advertised.listeners=INTERNAL_PLAINTEXT://
        192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093,EXTERNAL://
        [kafka_xmi]:9094 line in broker.properties file(path: /opt/kafka/
        config) and replace[kafka_xmi] with Kafka XMI IP
        ```

        ii. Comment:

        ```
        advertised.listeners=INTERNAL_PLAINTEXT://
        192.168.1.237:9092,INTERNAL_SSL://192.168.1.237:9093, EXTERNAL://
        10.196.84.46:9094 line.
        ```

    e. Run the below commands to restart Kraft and Kafka services:

    ```
    systemctl restart kafka
    ```

    After successful execution of the health check, Kafka is successfully set up on VM.

22. Service Setup
    a. Access the Service VM
    b. Navigate to the directory where the `setup-service.sh` script is located.
    c. Move the store Directory to the `/opt/` path using the following command:

    ```
    mv store /opt/
    ```

    d. Edit the Docker-compose file:
        i. Navigate to the `Services/ directory`.
        ii. Edit `cnidih_VM.yaml` file:
            i. <REPLACE WITH SOAM VIP> must be replaced with a valid active SOAM IP.

ii. Navigate to Protrace section and enable the following property `NFCONFIG_CLIENT_ENABLED` to **True**.

iii. Save and exit.

iii. Run the following command for the Service Setup Script:

```
./setup-service.sh
```

e. Configuration during execution: The script will prompt for several inputs during execution:

i. Enter Service IMI IP, Service XMI IP, Kafka IMI IP, and MySQL IMI IP.

> **Note**
>
> For IPv6 setups, the above IPs must be entered in square brackets ([]).

After these inputs are provided, the script will start the required services and proceed with the health check.

ii. Run the following command to verify if all services are running:

```
podman ps -a
```

Access the UI at: `https://<SERVICE XMI IP>/#/`.

This completes the setup for MySQL, Kafka, and Services. The deployment is now ready for use.

5.6 Post Installation Procedure

Kafka VM

> **Note**
>
> - By default, Kafka exposes the XSI IP on port 9094 to connect with DSR.
> - This procedure is only recommended if there is any issue connecting with XSI IP.

Perform the following procedure to update Kafka VM:

1. Log in to the Kafka VM.
2. Navigate to the Kafka configuration directory:

   ```
   cd /opt/kafka/config
   ```

3. Edit the `broker.properties` file:

   ```
   vi broker.properties
   ```

4. Locate the `advertised.listeners` property:

   ```
   advertised.listeners=EXTERNAL://<IP>:9094
   ```

5. Replace <IP> with the new IP (Kafka **xmi**, or **imi** if it is reachable from DSR).
6. Save the file and exit.
7. Perform the following command to restart the Kafka service status:

   ```
   systemctl restart kafka
   ```

8. Perform the following command to verify the Kafka service status:

   ```
   systemctl status kafka
   ```

   Expected result: The status should show active.

Service VM

This procedure is only applicable in the following cases:

- Case 1: User has not provides the DSR SOAM VIP during IDIH creation through VNFM in Swagger JSON.
- Case 2: User prefers to change the existing DSR SOAM VIP provided during creation. Perform the following procedure to update DSR SOAM VIP:
  1. Log in to the Service VM.
  2. Navigate to the `cd /opt/` directory:
  3. Edit the configuration file:

     ```
     vi cnidih_VM.yaml
     ```

  4. Inside the `nfconfig-manager` container section:
     a. Locate the property:

        ```
        NFCONFIG_PLUGIN_DSR_HOST
        ```

     b. Provide or replace the existing IP with the new one.
  5. Inside the `protraceprocessor` container section, ensure to set the following property`NFCONFIG_CLIENT_ENABLED` to **True**.

     > **Note**
     >
     > Verify it is set to true, not false.

  6. Save the file and exit.
  7. Perform the following command to restart the service:

     ```
     docker-compose -f /opt/cnidih_VM.yaml up -d
     ```

  8. If the SOAM VIP is reachable and appropriate, the `nfconfig` service and `protraceprocessor` services will operate as expected.

SSL Certificate Creation for IDIH

> **Note**
>
> Create your own certificates in case of expiration of provided certificate.

Kafka VM

1. Certificates are required in KeyStore and TrustStore format (PKCS or JKS).
2. Private key which is part of KeyStore must be encrypted.
3. One KeyStore and TrustStore file is required.

DSR (it acts as client for Kafka)

1. Certificates are required in pem format here.
2. Required files are: certificate, privatekey, CA file.
   Privatekey should be encrypted with password.
3. To upload the above files on DSR SOAM: from the **Main Menu**, go to **Diameter**, and **Troubleshooting with IDIH**, and then **Configuration**.

   > **Note**
   >
   > Same CA file must be used for Kafka and DSR Certificates.

Service VM

1. Certificates are required in KeyStore and TrustStore format (PKCS).
2. One KeyStore file and TrustStore file is required.
3. Same CA file can be used which is used while creating certificates for Kafka or different CA file also can be used.
4. Private key which is part of KeyStore must not be encrypted.
5. Certificate should contain the following fqdn's as SAN's (Subject Alternative Names):
   - idih.tekelec.com
   - tekelec.com
   - cnidih-portal
   - usermanagement
   - protraceprocessor
   - ttrdecoder
   - alarmmanagement

5.6.1 Enabling Security in IDIH

Enabling SSL in Kafka VM

Prerequisites: Refer to SSL Certificate creation for IDIH in the Post Installation Procedure section.

Perform the following procedure to populate SSL fields in `server.properties` file:

1. Log in to Kafka VM.
2. Create certificate directory from the following path if it does not exist.

   ```
   mkdir /opt/kafka/store/
   ```

3. Copy Kafka certificates to the `/opt/kafka/store` directory.
4. Update the permissions of `/opt/kafka/store` folder as well as the keystore and truststore files using the following command:
   - Assuming the name of KeyStore file is serverKeyStore.p12
   - Assuming the name of trustStore file is trustStore.p12

   ```
   chmod 775 /opt/kafka/store; chmod 775 /opt/kafka/store/serverKeyStore.p12;
   chmod 775 /opt/kafka/store/trustStore.p12
   ```

5. Navigate to `/opt/kafka/config` directory
6. Open `server.properties` from `vi server.properties`.
7. Modify `listener.security.protocol.map` property:
   a. There are three instances of `listener.security.protocol.map` in server.properties.
   b. Uncomment the one which has "SSL" for EXTERNAL listener and comment the other two.

      ```
      # Maps listener names to security protocols, the default is for them to
      be the same. See the config documentation for more details
      #listener.security.protocol.map=INTERNAL_PLAINTEXT:PLAINTEXT,PLAINTEXT:P
      LAINTEXT,INTERNAL_SSL:SSL,EXTERNAL:PLAINTEXT

      # Uncomment the below line and comment the other instances of
      "listener.security.protocol.map" to enable SSL for EXTERNAL Connectivity
      listener.security.protocol.map=INTERNAL_PLAINTEXT:PLAINTEXT,PLAINTEXT:PL
      AINTEXT,INTERNAL_SSL:SSL,EXTERNAL:SSL

      # Uncomment the below line and comment the other instances of
      "listener.security.protocol.map" to enable SASL_SSL for EXTERNAL
      Connectivity
      #listener.security.protocol.map=INTERNAL_PLAINTEXT:PLAINTEXT,PLAINTEXT:P
      LAINTEXT,INTERNAL_SSL:SSL,EXTERNAL:SASL_SSL
      ```

8. Uncomment and update the following SSL properties which are present at end of the file.

   ```
   # SSL
      ssl.protocol = TLS
      ssl.enabled.protocols=TLSv1.3
      ssl.keystore.type = PKCS12
      ssl.keystore.location = /opt/kafka/store/serverKeyStore.p12
      ssl.keystore.password = <keystore password>
      ssl.key.password = <key_password>
      ssl.truststore.type = PKCS12
      ssl.truststore.location = /opt/kafka/store/trustStore.p12
      ssl.truststore.password = <trust password>
   ```

```
ssl.cipher.suites=TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,TLS_CHACHA2
0_POLY1305_SHA256
   ssl.client.auth = required
```

9. Restart Kafka by running the following command:

   ```
   systemctl restart kafka
   ```

10. Kafka logs can be accessed at `/opt/kafka/kafkaservice.log` file.

> ⓘ **Note**
>
> For JKS type, update the following:
>
> - ssl.keystore.type,ssl.keystore.location
> - ssl.truststore.type,ssl.truststore.location accordingly.

Steps to enable SASL_SSL in Kafka VM

SASL_SSL is combination of SASL and SSL.

Prerequisites: SSL must be enabled, if SSL is not enabled then follow Steps to enable SSL in Kafka VM except the 7th and 9th point.

Perform the following procedure to populate `SASL_SSL` fields in `server.properties` file.

1. Login to Kafka VM.
2. Go to `/opt/kafka/config` and open the `server.properties` file.
3. Modify `listener.security.protocol.map` property.
   a. There are three instances of `listener.security.protocol.map` in `server.properties`.
   b. Uncomment the one which has `SASL_SSL` for EXTERNAL listener and comment the other two.

      ```
      # Maps listener names to security protocols, the default is for them to
      be the same. See the config documentation for more details
      #listener.security.protocol.map=INTERNAL_PLAINTEXT:PLAINTEXT,PLAINTEXT:P
      LAINTEXT,INTERNAL_SSL:SSL,EXTERNAL:PLAINTEXT

      # Uncomment the below line and comment the other instances of
      "listener.security.protocol.map" to enable SSL for EXTERNAL Connectivity
      #listener.security.protocol.map=INTERNAL_PLAINTEXT:PLAINTEXT,PLAINTEXT:P
      LAINTEXT,INTERNAL_SSL:SSL,EXTERNAL:SSL

      # Uncomment the below line and comment the other instances of
      "listener.security.protocol.map" to enable SASL_SSL for EXTERNAL
      Connectivity
      listener.security.protocol.map=INTERNAL_PLAINTEXT:PLAINTEXT,PLAINTEXT:PL
      AINTEXT,INTERNAL_SSL:SSL,EXTERNAL:SASL_SSL
      ```

4. Uncomment the following property:

   ```
   sasl.enabled.mechanisms=PLAIN
   ```

5. Go to `/opt/kafka/store` path.
6. Create a file named `kafka_server_jaas.conf` file using the following template:

   ```
   KafkaServer {
   org.apache.kafka.common.security.plain.PlainLoginModule required
   user_username1="user1password"
   user_username2="user2password"
   user_username3="user3password"
   user_username4="user4password"
   .
   .
   .
   user_usernameN="userNpassword";
   };



   Example :
   KafkaServer {
   org.apache.kafka.common.security.plain.PlainLoginModule required
   user_idihuser1="changeme"
   user_idihuser2="changeme"
   user_idihuser3="changeme";
   };
   ```

   > **Note**
   >
   > - The username accepts only alphanumeric characters. Range: the length of the username must be between 8 and 64 characters.
   > - The password accepts any characters. Range: the length of the password must be between 8 and 64 characters.

7. Update the permissions of file so that kafka process will have read access and restrict the other users.
8. Perform the following command to export:

   ```
   export KAFKA_OPTS="-Djava.security.auth.login.config=/opt/kafka/store/
   kafka_server_jaas.conf"
   ```

9. Perform the following command to restart Kafka:

   ```
   systemctl restart kafka
   ```

10. Kafka logs can be accessed at `/opt/kafka/kafkaservice.log` file.

Enable SSL for internal communication in Service VM

Prerequisites: Refer to SSL Certificate creation for IDIH in the Post Installation Procedure section.

Perform the following procedure to enable SSL for internal communication in Service VM:

1. Log in to Service VM.
2. Copy the files to the following path `/opt/store` in service VM.
3. Update the permissions of `/opt/store` folder as well as the keystore and truststore files using the following command:

   ```
   chmod 775 /opt/store; chmod 775 /opt/store/serverKeyStore.p12; chmod
   775 /opt/store/trustStore.p12
   ```

4. Go to opt directory `cd /opt`.
5. Edit docker compose file:

   ```
   vi cnidih_VM.yaml
   ```

6. The password for the keystore and truststore is provided by default, if the user changes the files, they can modify the password in the sections below:

   ```
   MICRONAUT_SERVER_SSL_KEY_STORE_PASSWORD
   MICRONAUT_SERVER_SSL_TRUST_STORE_PASSWORD
   MICRONAUT_HTTP_CLIENT_SSL_KEY_STORE_PASSWORD
   MICRONAUT_HTTP_CLIENT_SSL_TRUST_STORE_PASSWORD
   ```

Service VM Alert Manager TLS Config

1. On the service VM, navigate to the `/opt` path and then to the `alertmanager` directory, within this directory, you will find a file named `alertmanager.yaml`.
2. Open the file, comment out the line for non-TLS communication, and uncomment the lines for TLS configuration, as shown below:

   ```
   - url: 'http://alarmmanagement:8092/api/cnidih/alarmmanagement/v1/alarms'
   # below four lines is for tls
   #- url: 'https://alarmmanagement:8092/api/cnidih/alarmmanagement/v1/alarms'
   # http_config:
   # tls_config:
   # insecure_skip_verify: true
   ```

3. After making the changes, run the following command to list all the containers:

   ```
   podman ps -a
   ```

4. Identify the Alertmanager container and remove it by running the following command:

   ```
   podman rm -f <container id>
   ```

5. Run the following command to restart the services

```
docker-compose -f cnidih_VM.yaml up -d
```

> **Note**
>
> Ensure the password for certificates has been updated accordingly in the `cnidih_VM.yaml` file.

Validation

- Access Kafka using client certificates.
- Access the IDIH portal with `https://`.

5.6.2 SNMP Configuration In Alertmanager IDIH

SNMP Configuration

In the following command, provide valid ip and port in docker compose file

```
snmp_notifier:
    image: occnidih-docker.dockerhub-iad.oci.oraclecorp.com/snmp-
notifier:v2.1.0
    privileged: true
    volumes:
      - ./snmp/:/templates/
    environment:
      # Required for SNMP v3
      - SNMP_NOTIFIER_AUTH_USERNAME=snmp_user
      - SNMP_NOTIFIER_AUTH_PASSWORD=P@ssw0rd
      - SNMP_NOTIFIER_PRIV_PASSWORD=changeme
    command:
      - "--trap.description-template=/templates/description-template.tpl"
      - "--snmp.destination=[service_xmi]:162"
      - "--snmp.retries=2"
      - "--snmp.timeout=5s"
      - "--snmp.version=V3"
      - "--snmp.authentication-enabled"
      - "--snmp.authentication-protocol=SHA"
      - "--snmp.private-enabled"
      - "--snmp.private-protocol=AES"
    ports:
      - "0.0.0.0:9464:9464"
      - "[::]:9464:9464"
    logging:
      options:
        max-size: "10m" # Limits each log file to 10 MB
        max-file: "3" # Retains up to 3 rotated log files
    networks:
      - cnidih-network
```

Update the `alertmanager.yaml` to ensure snmp is configured appropriately for sending data to respective NMS.

```
global:
  resolve_timeout: 5m

receivers:
  - name: default-receiver
    webhook_configs:
      - url: http://snmp_notifier:9464/alerts
  - name: alarmmanagement-receiver
    webhook_configs:
      # below line is for non tls
      - url: 'http://alarmmanagement:8092/api/cnidih/alarmmanagement/v1/
alarms'
        # below four lines is for tls
        #- url: 'https://alarmmanagement:8092/api/cnidih/alarmmanagement/v1/
alarms'
        #  http_config:
        #    tls_config:
        #      insecure_skip_verify: true


route:
  group_by:
    - namespace
  group_interval: 5m
  group_wait: 30s
  receiver: default-receiver
  repeat_interval: 12h
  routes:
    - matchers:
        - alertname = "Watchdog"
      receiver: default-receiver
    - matchers:
        - app =~ "tdrstorage|ttrdecoder|protrace.*|protraceprocessor|
nfconfig.*|nfconfigmanager|protocoldecoder|alarmmanagement|apigateway|
cnidihportal|cnidih*|portal*|logauditmanager|logaudit*|usermanagement|kafka-
broker|kafka*|zookeeper*"
      receiver: default-receiver
```

5.7 iDIH Configuration to Configure the SSO Domain

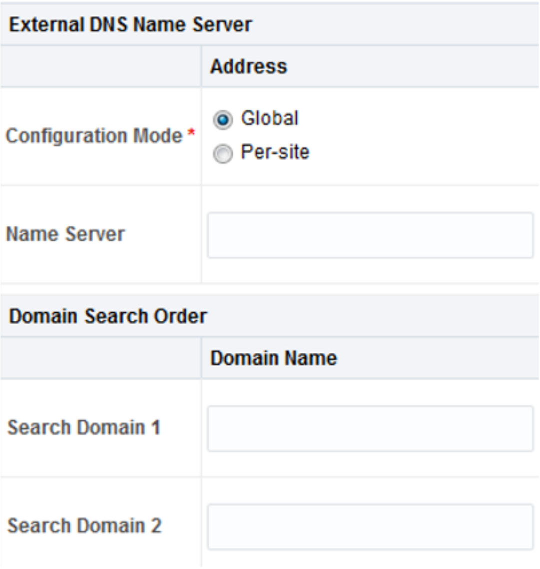
This procedure configures the SSO domain for iDIH:

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. Log in as the `admusr` user.
2. In NOAM VIP GUI, configure DNS:
   a. Navigate to **Administration**, and then **Remote Servers**, and then **DNS Configuration**.
   b. Select the NOAM tab.
   c. Configure values for the following fields:

Domain Name

Name Server

Search Domain 1



External DNS Name Server

	Address
Configuration Mode *	● Global ○ Per-site
Name Server	

Domain Search Order

	Domain Name
Search Domain 1	
Search Domain 2	

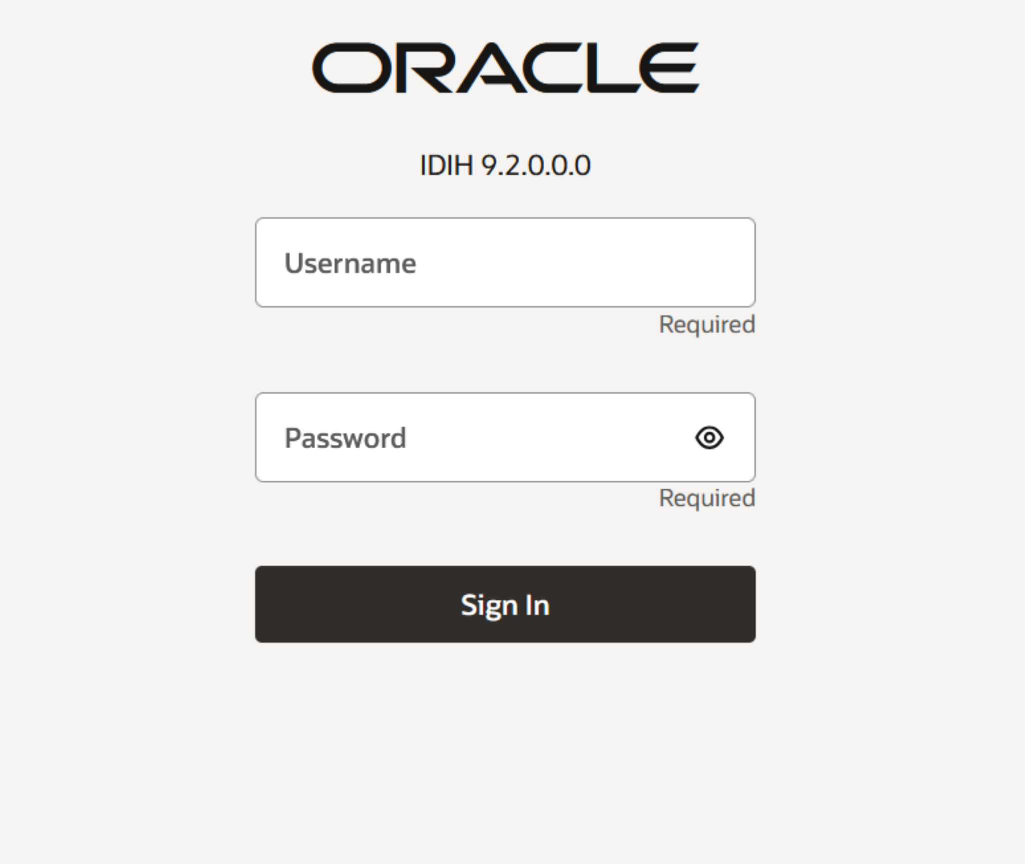
   d. If values have already been configured, click **Cancel**. Otherwise configure the values and click **OK**.

3. In NOAM VIP GUI, establish SSO local zone.
   a. Navigate to **Access Control**, and then **Certification Management**.
   b. Click **Establish SSO Zone**.
   c. Type a value for **Zone Name**.
   d. Click **OK**.
   Information for the new certificate type of SSO local displays.
   e. Click **Report**.
   The Certificate Report appears.
   f. Select and copy the encoded certificate text to the clipboard for future access.
   Example of Certificate Report:

```
-----BEGIN CERTIFICATE-----
MIICKzCCAdWgAwIBAgIJAOVfSLNc3CeJMA0GCSqGSIb3DQEBCwUAMHExCzAJBgNVBAYTAlVT
MQswCQYDVQQIDAJOQzEQMA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UECgwGT3JhY2xlMQswCQYD
VQQLDAJQVjEQMA4GA1UEAwwHTGliZXJ0eTETMBEGCSqGSIb3DQEJARYEdGVzdDAeFw0xNTA1
MDQxNDIzNTRaFw0xNjA1MDMxNDIzNTRaMHExCzAJBgNVBAYTAlVTMQswCQYDVQQIDAJOQzEQ
MA4GA1UEBwwHUmFsZWlnaDEPMA0GA1UECgwGT3JhY2xlMQswCQYDVQQLDAJQVjEQMA4GA1UE
AwwHTGliZXJ0eTETMBEGCSqGSIb3DQEJARYEdGVzdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgC
QQCZ/MpkhlvMP/
iJs5xDO2MwxJm3jYim43H8gR9pfBTMNP6L9kluJYi+2T0hngJFQLpIn6SK6pXnuAGYf/
vDWfqPAgMBAAGjUDBOMB0GA1UdDgQWBBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAfBgNVHSMEGD
AWgBS6IzIOLP1gizQ6+BERr8Fo2XyDVDAMBgNVHRMEBTADAQH/
MA0GCSqGSIb3DQEBCwUAA0EAOwIqBMEQyvfvt38r/
yfgIx3w5dN8SBwHjHC5TpJrHV6UzFlg5dfzoLz7ditjGOhWJ9l9VRw39LQ8lKFp7SMXwA==
-----END CERTIFICATE-----
```

4. Log in as adminuser.
   a. Establish a GUI session on the iDIH application server, using the xmi IP address `https://<app server IP>`
   b. Log in as the `idihadmin` user.

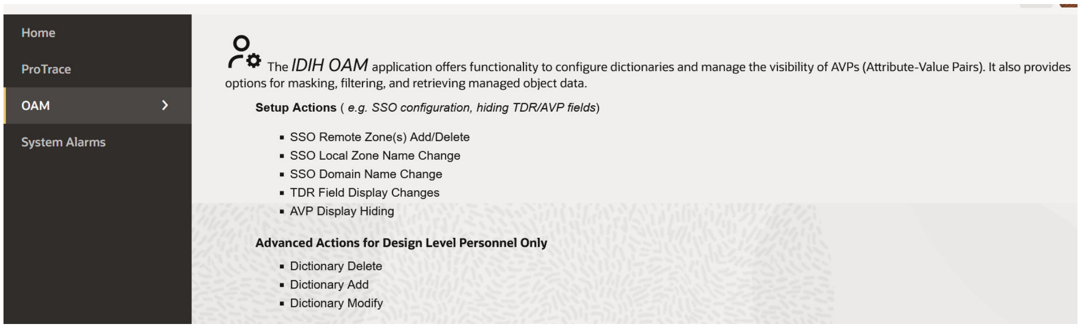
Figure 5-43 IDIH Login



5. In IDIH Application server GUI, launch the OAM portal.

   Navigate to the OAM portal icon to start the OAM web application.

Figure 5-44 OAM



The *IDIH OAM* application offers functionality to configure dictionaries and manage the visibility of AVPs (Attribute-Value Pairs). It also provides options for masking, filtering, and retrieving managed object data.

Setup Actions (*e.g. SSO configuration, hiding TDR/AVP fields*)

- SSO Remote Zone(s) Add/Delete
- SSO Local Zone Name Change
- SSO Domain Name Change
- TDR Field Display Changes
- AVP Display Hiding

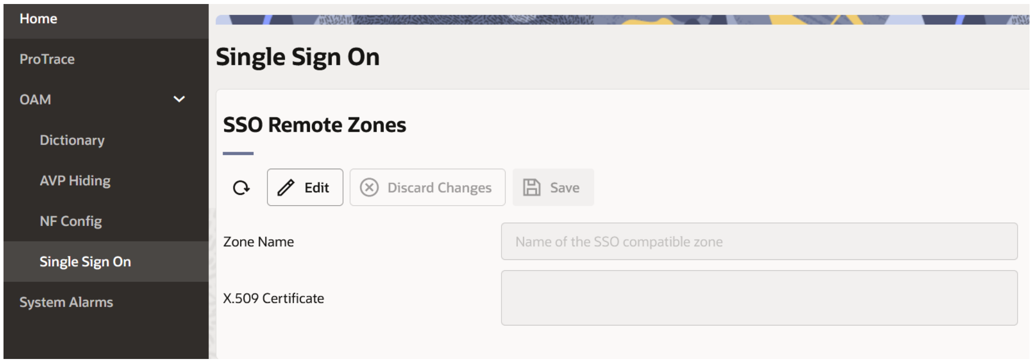
Advanced Actions for Design Level Personnel Only

- Dictionary Delete
- Dictionary Add
- Dictionary Modify

6. In iDIH Application server GUI, configure the SSO domain.

a. Navigate to **OAM**, and then **Single Sign On**.

Figure 5-45 SSO



b. Select **SSO Parameters** tab.

c. Click **Edit Value** icon.

d. Type a value for the **Domain Name**.

> **Note**
>
> This should be the same domain name assigned in the DSR NOAM DNS Configuration (step 2).

e. Click **Save** icon.

f. Click **Refresh** icon to display data saved for the remote zone.

7. In iDIH Application server GUI, configure the SSO Remote Zone.
   a. Navigate to **System**, and then **Single Sign On**.
   b. Select **SSO Zones** tab.
   c. Click **Add** icon.
   d. Type a value for field **Remote Name**.
   e. For field X.509 Certificate, paste the encoded certificate text from the clipboard that was previously copied from the DSR NOAM.
   f. Click **Save**.
   g. Click **Refresh** to display data saved for the remote zone.

> **Note**
>
> To configure IDIH with DSR, see *Integrated Diameter Intelligence Hub User guide*.

6

Postinstallation Activities

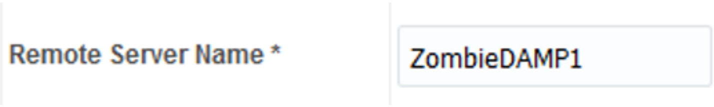
6.1 Configure ComAgent Connections

This procedure configures ComAgent connections on DSR for use in the FABR application.

Prerequisites:
FABR application is activated.

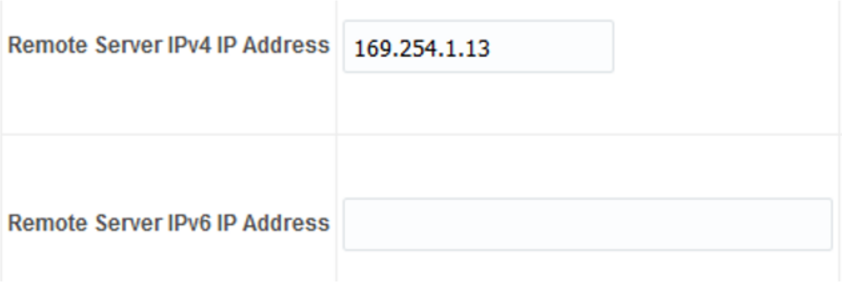
> ⓘ **Note**
>
> For more information, see *SDS Cloud Installation and Configuration Guide*.

1. Log in to SDS NOAM VIP GUI.
   a. 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.
   b. Log in as the `admusr` user.
2. In SDS NOAM VIP GUI, configure remote server IP address.
   a. Navigate to **Communication Agent**, and then **Configuration**, and then **Remote Servers**.
   b. Click **Insert**.
3. In SDS NOAM VIP GUI, configure remote server IP address.
   a. Type `Remote Server Name` for the DSR MP server.



Remote Server Name *	ZombieDAMP1

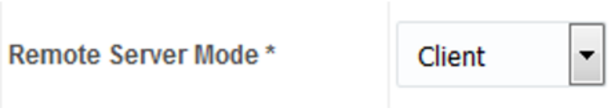
   b. Type the `Remote Server` IMI IP address.



Remote Server IPv4 IP Address	169.254.1.13
Remote Server IPv6 IP Address	

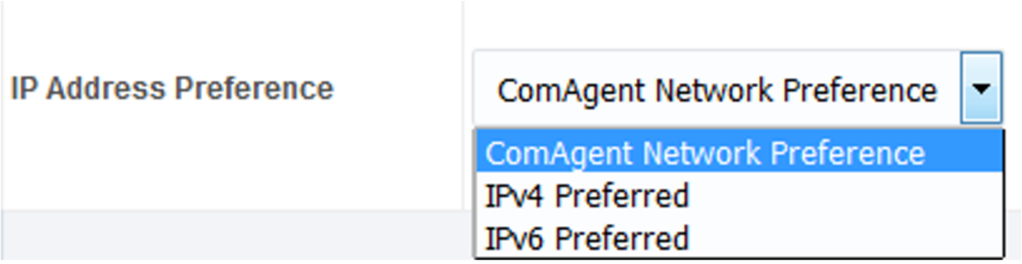
> **Note**
>
> This should be the IMI IP address of the DAMP server.

c. Select **Client** for the Remote Server Mode from the list.



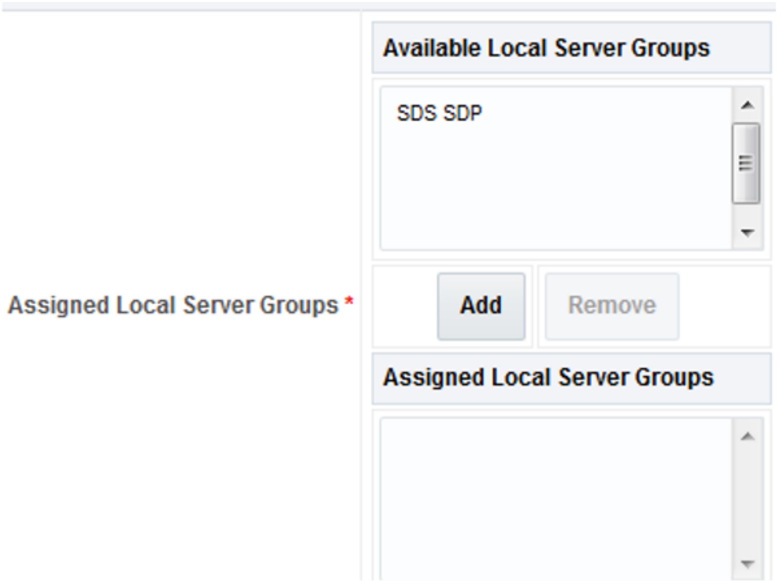
Remote Server Mode * Client

d. Select **IP Address Preference** (ComAgent Network Preference, IPv4, or IPv6) from the list.

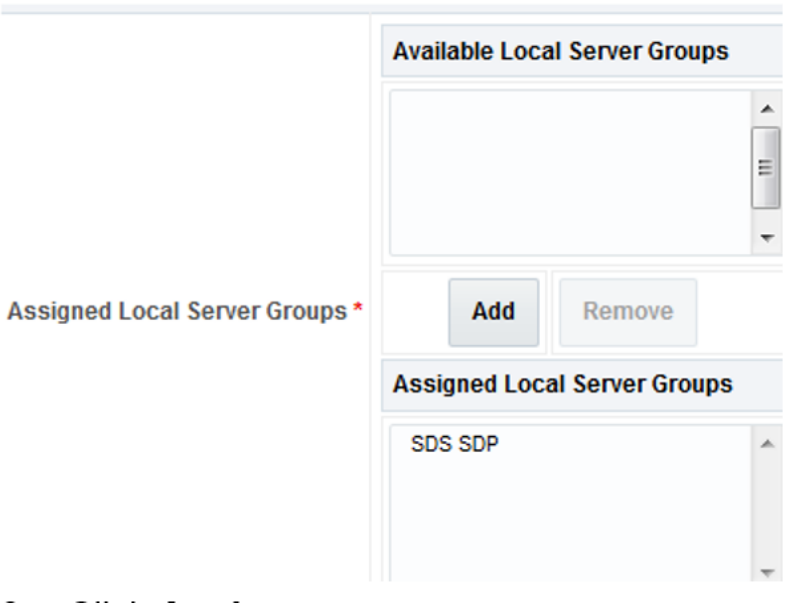


IP Address Preference ComAgent Network Preference

e. Select the **Local Server Group** from the available SDS DP server groups and click **Add** to assign.



Assigned Local Server Groups *



Assigned Local Server Groups *

SDS SDP

f. Click **Apply**.

> **Note**
>
> Repeat steps 2-3 for each remote MP in the same SOAM NE.

4. Log in to DSR NOAM VIP GUI.
   a. 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.
   b. Log in as the `guiadmin` user.
5. In DSR NOAM VIP GUI, configure remote server IP address.
   a. Navigate to **Communication Agent**, and then **Configuration**, and then **Remote Servers**.
   b. Click **Insert**.
6. In DSR NOAM VIP GUI, configure remote server IP address.
   a. Type `Remote Server Name` for the DSR MP server.
   b. Type the `Remote Server` IMI IP address.

   > **Note**
   >
   > This should be the IMI IP address of the DP server.

   c. Select **Server** for the Remote Server Mode from the list.
   d. Select **IP Address Preference** (ComAgent Network Preference, IPv4, or IPv6) from the list.
   e. Select the **Local Server Group** from the available DSR MP server groups and click **Add** to assign.

f. Click **Apply**.

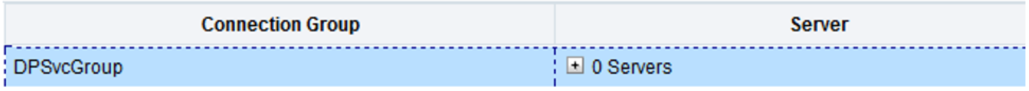
> **Note**
>
> Repeat steps 5-6 for each remote DP in the same SOAM NE.

7. In DSR NOAM VIP GUI, configure connection groups.

   a. Navigate to **Communication Agent**, and then **Configuration**, and then **Connection Groups**.

8. In DSR NOAM VIP GUI, edit connection groups.

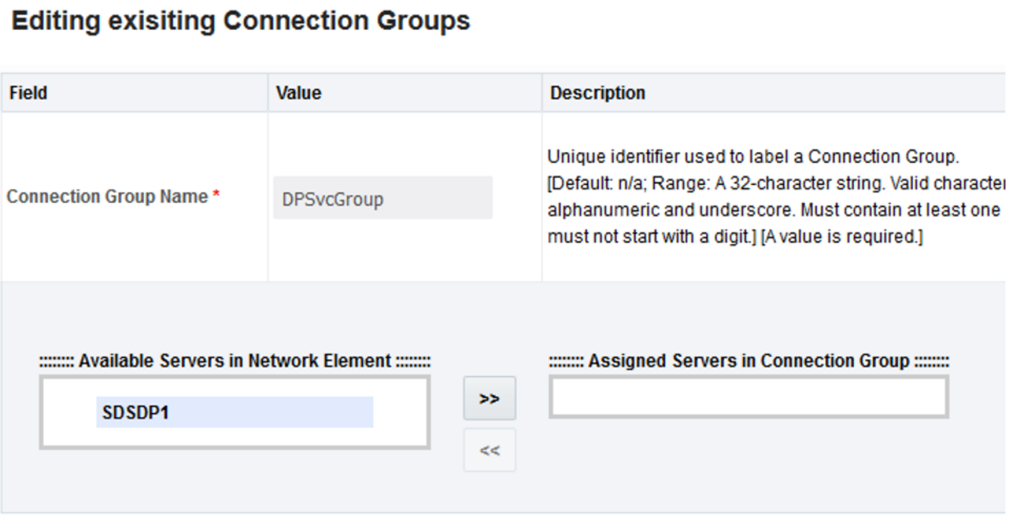
   a. Select the **DPSvcGroup** connection group.



Connection Group	Server
DPSvcGroup	⊞ 0 Servers

   b. Click **Edit**.

   c. Select the `DP Servers` from the Available Servers in Network Element list and click **>>** to assign.



Editing exisiting Connection Groups

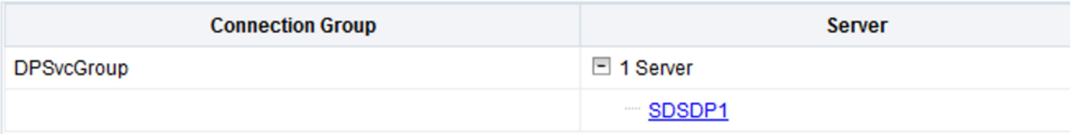
Field	Value	Description
Connection Group Name *	DPSvcGroup	Unique identifier used to label a Connection Group. [Default: n/a; Range: A 32-character string. Valid characte alphanumeric and underscore. Must contain at least one must not start with a digit.] [A value is required.]

:::::::: Available Servers in Network Element :::::::: SDSDP1

:::::::: Assigned Servers in Connection Group ::::::::

   d. Click **OK**.

9. In DSR NOAM VIP GUI, verify the correct number of servers are in the connection group.



Connection Group	Server
DPSvcGroup	⊟ 1 Server
	SDSDP1

6.2 Complete PCA Configuration

This procedure completes PCA configuration. This is an optional procedure.

Prerequisites:

PCA application must be activated.

> ⓘ **Note**
>
> Refer to "Section PCA Configuration" in *DSR PCA Activation Guide* for the steps required to complete PCA configuration.

6.3 Backups and Disaster Prevention

This procedure provides information on backups and disaster prevention.

Prerequisites:
DSR and optional sub-systems are installed configured.

1. Backup from VIM.

   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.

   > ⓘ **Note**
   >
   > Perform the following steps also to back up the NOAM and SOAM database.

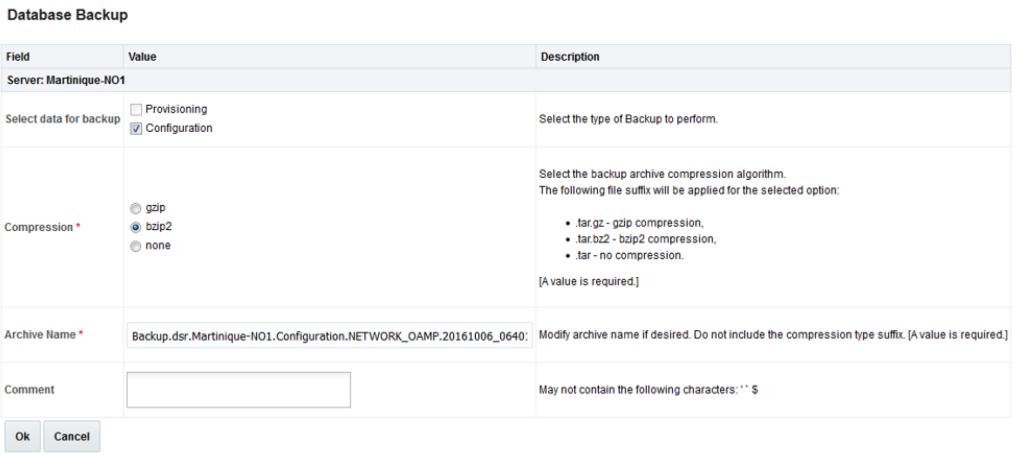
2. Identify Backup Server.

   Identify an external server to be used as a backup server for the following steps. The server should not be co-located with any of the following items:

   - Cloud Infrastructure Manager Server/Controller
   - DSR NOAM
   - DSR SOAM

3. Log in to NOAM/SOAM VIP.
   a. Establish a GUI session on the NOAM or SOAM server by using the VIP IP address of the NOAM or SOAM server.
   b. Open the web browser and enter a URL `http://<Primary_NOAM/SOAM_VIP_IP_Address>`
   c. Login as the **guiadmin** user.

4. In NOAM/SOAM VIP, perform backup configuration data for the system.
   a. Navigate to **Main Menu**, and then **Status & Manage**, and then **Database**.
   b. Select the active NOAM server and click **Backup**.
   c. Ensure the **Configuration** checkbox is marked.



Database Backup

Field	Value	Description
Server: Martinique-NO1		
Select data for backup	□ Provisioning ☑ Configuration	Select the type of Backup to perform.
Compression *	○ gzip ● bzip2 ○ none	Select the backup archive compression algorithm. The following file suffix will be applied for the selected option: • .tar.gz - gzip compression, • .tar.bz2 - bzip2 compression, • .tar - no compression. [A value is required.]
Archive Name *	Backup.dsr.Martinique-NO1.Configuration.NETWORK_OAMP.20161006_0640:	Modify archive name if desired. Do not include the compression type suffix. [A value is required.]
Comment		May not contain the following characters: ' ` $

d. Enter a filename for the backup and click **OK**.

5. In NOAM/SOAM VIP, verify the backup file existence.

   a. Navigate to **Main Menu**, and then **Status & Manage**, and then **Files**.

   b. Select the active NOAM or SOAM tab.
   The files on this server are displayed.

   c. Verify the existence of the backup file.

6. In NOAM/SOAM VIP, download the file to a local machine.

   a. From the previous step, select the backup file.

   b. Click **Download**.

   c. Click **OK**.

> **Note**
>
> - Transfer the backed up image to a secure location identified in step 2 where the server backup files are fetched in case of system disaster recovery.
> - Repeat Steps 3 through 6 to back up the active SOAM.

6.4 Configure Port Security (KVM/OpenStack Only)

This procedure configures port security on TSA.

Prerequisites:

- Perform "**Enable the Neutron port security extension**".
- We require this extension to disable the Neutron anti-spoofing filter rules for a given port.
- Refer to Disable Port Security where this is discussed.

1. IPFE with TSA only. Remove allowable address pair security on IPFE XSI network and DAMP XSI interfaces on IPFE and MP instances.

   If stacks are deployed using HEAT template, follow this step.

   a. Determine the TSA IP address used in Configure IP Front End.

b. Determine the corresponding XSI interface IP address assigned to that TSA used in Configure IP Front End.

c. Determine the XSI IP address of IPFE used in Configure IP Front End.

d. Log in to the OpenStack control node as the **admusr** user.

e. Source the tenant user credentials.

f. Determine the port ID of the XSI interface IP address.

```
$ neutron port-list -F id -F fixed_ips | grep <XSI network>
```

> **Note**
>
> <port ID> is the value in first column of the output to this command.

g. Remove allowed_address_pairs:

```
$ neutron port-update <Port ID> --no-allowed-address-pairs
```

> **Note**
>
> Run neutron port-show command to verify allowed_address_pairs attribute is empty.

2. IPFE with TSA only. Remove port security on TSA XSI network interfaces on IPFE and MP instances.

   If using IPFE with Target Set Addresses (TSA).

   a. Determine the TSA IP address as used in Configure IP Front End section.

   b. Determine the corresponding XSI interface IP address as used in Configure IP Front End section.

   c. Log in to the OpenStack control node as the `admusr` user.

   d. Source the tenant user credentials.

   e. Determine security groups associated with the IPFE instance.

```
$ nova list-secgroup <VM instance ID>
```

> **Note**
>
> <VM instance ID> can be queried from the output of `nova list` command in the ID column for the given VM.

   f. Save the ID and names of the listed security groups for later use.

   g. Remove all listed security groups.

```
$ nova remove-secgroup <VM instance ID> <Security group ID>
```

> **Note**
>
> Use the <VM instance ID> and <Security group ID> as noted down in the step-f above.

Alternatively, use the following syntax:

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

h. Determine the port ID of the XSI interface IP address from step b above.

```
$ neutron port-list -F id -F fixed_ips | grep <instance IP on TSA/XSI
network>
```

> **Note**
>
> <port ID> is the value in first column of the output to this command.

i. Disable port security for the port found in step g.

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

j. Re-enable port security for all the interfaces not on the TSA/XSI port used in step i, including XMI, IMI, and others.

k. Determine the port IDs of the instance IP addresses not associated with the TSA/XSI network.

```
$ neutron port-list -F id -F fixed_ips | grep <instance IP not on
TSA/XSI network>
```

l. For each of the non TSA/XSI instance ports perform the following command for each of the security groups from step f.

```
$ neutron port-update <Port ID> --security-group <Security group ID>
```

> **Note**
>
> Use the <Security Group ID> as noted down in the step f above.

6.5 Enable/Disable DTLS (SCTP Diameter Connections Only)

This procedure prepares clients before configuring SCTP Diameter connections.

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.

- `https://access.redhat.com/security/cve/CVE-2015-1421`
- `https://access.redhat.com/security/cve/CVE-2014-5077`

Run the procedures in *DSR DTLS Feature Activation Procedure* to disable or enable the DTLS feature.

6.6 Shared Secret Encryption Key Revocation (RADIUS Only)

This procedure changes the shared secret encryption key on DSR RADIUS setup.

Refer to "RADIUS Shared Secret Key revocation MOP" to change the encryption key on the DSR installed setup. Refer to "DSR RADIUS Shared Secret Encryption Key Revocation" MOP MO008572.

> **Note**
>
> It is highly recommended to change the key after installation due to security reasons.

6.7 DSR Performance Tuning

This procedure changes tuning parameters for the system to achieve better performance. This is an optional step.

Refer to Performance Tuning Recommended for performance tuning on DSR.

6.8 Change NOAM/SOAM Profile for Increased MP Capacity on a Virtualized Environment

This procedure describes how to change NOAM and SOAM VM profile when the MP capacity is increased on OpenStack and VMware.

1. Log in to OpenStack/VMware.
    - To change the VM profile when the MP capacity is increased on OpenStack, log in to Openstack GUI horizon dashboard.
    - To change the VM profile when the MP capacity is increased on VMware, log in to VM manager.
2. Refer to the section "Change NOAM/SOAM VM Profile for Increased MP Capacity" in *DSR Cloud Upgrade Guide*.

6.9 Resolve False Alarms for DA MP and vSTP MP

The following critical alarms raised for DA MP (Diameter Agent Message Processor), Virtual Session Transfer Protocol Message Processor (vSTP MP) in DSR or vSTP for combined deployments with multiple sites can be ignored:

- 25500 - No DA MP Leader Detected
- 70371 - No vSTP MP Leader Detected

If required, perform the following procedure to resolve the above alarms:

1. On DSR SOAM, run the following commands:

   ```
   iset -fcntl=off PmControl where "procTag='vstpoam'"
   iset -fcntl=respawn PmControl where "procTag='dsroam'"
   ```

2. On vSTP SOAM, run the following commands:

   ```
   iset -fcntl=off PmControl where "procTag='dsroam'"
   iset -fcntl=respawn PmControl where "procTag='vstpoam'"
   ```

> ⓘ **Note**
>
> In future, system restarts, these alarms will not reappear.

6.10 Workaround for Configuring GUI and MMI Using Label Format for FQDN/Realm

For the users who prefer to configure with a single label format instead of the label.label format for FQDN/Realm, perform the following procedure for GUI and MMI configuration changes:

> ⓘ **Note**
>
> By default, thecode is compliant.

1. Navigate to the `cd /usr/TKLC/dpi/prod/maint/scripts/` folder.
2. Run the following command:

   ```
   sudo ./rfcRealmFqdn.sh
   ```

3. Select an option from the list and proceed with the FQDN/Realm configuration:
   a. Non-Compliant: Allow RFC (Request for Comments) Non-Compliant label format.
   b. Compliant: Allow RFC Compliant label format.
   c. Quit

   > ⓘ **Note**
   >
   > To continue with the switchover, this manual step must be performed on every OAM server.

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.

Example for Network Element XML File

```
<?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>
```

> **Note**
>
> NetworkElement Name must be unique while creating multiple Network Element.

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 B-1 List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
UTC	Universal Time Coordinated	UTC-00
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
America/Mexico City	Central Time — most locations	UTC-06
Africa/Monrousing		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

Table B-1 (Cont.) List of Selected Time Zone Values

Time Zone Value	Description	Universal Time Code (UTC) Offset
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

C

Common KVM/OpenStack Tasks

C.1 Create a Network Port

Perform the following steps to create the network ports for the NO network interfaces:

1. 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.

2. Determine the IP address for the interface.

   For eth0, the IP might be 10.x.x.157
   For eth1, the IP might be 192.168.x.157

3. Identify the neutron network ID associated with each IP/interface using the neutron command line tool.

   ```
   $ neutron net-list
   ```

4. Identify the neutron subnet ID associated with each IP/interface using the neutron command line tool.

   ```
   $ neutron subnet-list
   ```

5. Create the network port using the neutron command line tool, being sure to choose an informative name. Note the use of the subnet ID and the network ID (final argument).

   Port names are usually a combination of instance name and network name.
   NO1-xmi

   SO2-imi

   MP5-xsi2

   The ports must be owned by the DSR tenant user, not the admin user. Either source the credentials of the DSR tenant user or use the DSR tenant user ID as the value for the —**tenant-id** argument.

   ```
   $ . keystonerc_dsr_user
   $ keystone user-list
   $ neutron port-create --name=NO1-xmi –-tenant-id <tenant id> --fixed-ip
   subnet_id=<subnet id>,ip_address=10.x.x.157 <network id>
   $ neutron port-create --name=NO1-imi --tenant-id <tenant id> --fixed-ip
   subnet_id=<subnet id>,ip_address=192.168.x.157 <network id>
   ```

   View your newly created ports using the neutron tool.

   ```
   $ neutron port-list
   ```

C.2 Create and Boot OpenStack Instance

Perform the following steps to create a VM instance from a glance image.

1. Get the following configuration values.

   The image ID.

   ```
   $ glance image-list
   ```

   The flavor ID.

   ```
   $ nova flavor-list
   ```

   The network ID(s).

   ```
   $ neutron net-list
   ```

   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. Number of IP/ interfaces for each VM type must conform with the DSR Network to Device Assignments defined in *DSR Cloud Benchmarking Guide*.

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

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

   View the newly created instance using the nova tool.

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

   The VM takes approximately 5 minutes to boot. At this point, the VM has no configured network interfaces and can only be accessed by the Horizon console tool.

C.3 Configure Networking for OpenStack Instance

Perform the following steps to verify or configure Networking for OpenStack Instance.

1. Check if the interface is configured automatically.
2. If DHCP is enabled on Neutron subnet, VM configures the VNIC with the IP address. To verify, ping the XMI IP address provided with the nova boot command:

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

   If the ping is successful, ignore the next part to configure the interface manually.

   Manually configure the interface, if not already done (optional).

   a. Log in to the **Horizon** GUI as the DSR tenant user.
   b. Go to the **Compute/Instances** section.
   c. Click on the **Name** field of the newly created instance.
   d. Select the **Console** tab.
   e. Log in as the **admusr** user.
   f. Configure the network interfaces, conforming with the interface-to-network mappings defined in *DSR Cloud Benchmarking Guide*.

      ```
      $ sudo netAdm add --onboot=yes --device=eth0 --address=<xmi ip> --
      netmask=<xmi net mask>
      $ sudo netAdm add --route=default --device=eth0 --gateway=<xmi gateway
      ip>
      ```

      Under some circumstances, it may be necessary to configure as many as 6 or more interfaces.
3. Reboot the VM. It takes approximately 5 minutes for the VM to complete rebooting.

   ```
   $ sudo init 6
   ```

   The new VM should now be accessible using both network and Horizon console.

D

Common OVM Manager Tasks (CLI)

D.1 Set Up the Server

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.

1. Log in to the OVM-M command line interface.

   ```
   ssh –l admin <OVM-M IP> -p 1000
   ```

   Example:

   ```
   [root@manager01 ~]# ssh -l admin 10.240.16.138 -p 10000
   admin@10.240.16.138's password:
   ```

2. In OVM-M CLI: Discover Oracle VM server.

   ```
   discoverServer ipAddress=value password=value takeOwnership= { Yes | No }
   ```

   Example:

   ```
   OVM>discoverServer ipAddress=10.240.16.139 password=password
   takeOwnership=Yes
   ```

3. In OVM-M CLI, create an ethernet-based network with the VM role.

   ```
   create Network [ roles= { MANAGEMENT | LIVE_MIGRATE | CLUSTER_HEARTBEAT |
   VIRTUAL_MACHINE | STORAGE } ] name=value [ description=value ] [ on Server
   instance ]
   ```

   Example:

   ```
   OVM>create Network name=XMI roles=VIRTUAL_MACHINE
   ```

4. In OVM-M CLI, add a port from each Oracle VM server to the network.

   > ⓘ **Note**
   >
   > Skip this step and proceed to step 5 for bonded interfaces.

   a. Find the ID of an Ethernet port.

      ```
      OVM> show Server name=MyServer1
      ...
      ```

```
Ethernet Port 1 = 0004fb00002000007711332ff75857ee
[eth0 on MyServer3.virtlab.info]
Ethernet Port 2 = 0004fb0000200000d2e7d2d352a6654e
[eth1 on MyServer3.virtlab.info]
Ethernet Port 3 = 0004fb0000200000c12192a08f2236e4
[eth2 on MyServer3.virtlab.info]
```

b. Add a port from each Oracle VM Server to the network.

```
OVM>add Port instance to { BondPort | Network } instance
```

Example:

```
OVM>add Port id=0004fb0000200000d2e7d2d352a6654e to Network
name=MyVMNetwork
```

5. In OVM-M CLI, create Bondport (For Bonded Interfaces).

a. Find the ID of an Ethernet port.

```
OVM>list Port
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
```

b. Create Bondport on required interfaces.

```
OVM>create BondPort
ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0
d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server
name=compute01.test.com
```

Command:

```
create BondPort
ethernetPorts="0004fb0000200000b1dceeb39006d839,0004fb0000200000fce443e0
d30cd3d5" mode=ACTIVE_PASSIVE mtu=1500 name=bond1 on Server
name=compute01.test.com
Status: Success
```

6. In OVM-M CLI, add VLAN Interface to network (for VLAN tagged networks).

a. Find the ID of an Ethernet port.

```
OVM>list BondPort
Command: list BondPort
Status: Success
Time: 2016-08-22 04:38:22,327 EDT
```

```
Data:
id:0004fb00002000005a45a0761813d512 name:bond1
id:0004fb0000200000645cfc865736cea8 name:bond0 on compute01.test.com
```

b. Create VLAN interface.

```
OVM>create VlanInterface vlanId=43 name=bond1.43 on BondPort
id=0004fb00002000005a45a0761813d512


create VlanInterface vlanId=43 name=bond1.43 on BondPort
id=0004fb00002000005a45a0761813d512
Status: Success
```

c. Add remaining VLAN interfaces to the same bond accordingly, like:

```
OVM>create VlanInterface vlanId=44 name=bond1.44 on BondPort
id=0004fb00002000005a45a0761813d512
OVM>create VlanInterface vlanId=30 name=bond1.30 on BondPort
id=0004fb00002000005a45a0761813d512
OVM>create VlanInterface vlanId=31 name=bond1.31 on BondPort
id=0004fb00002000005a45a0761813d512
```

d. Add VLAN interfaces to network.

```
OVM>add VlanInterface name=bond1.43 to Network name=XMI
Command: add VlanInterface name=bond1.43 to Network name=XMI
Status: Success
Time: 2016-08-22 05:14:29,321 EDT
JobId: 1471857258238
OVM>add VlanInterface name=bond1.44 to Network name=IMI
Command: add VlanInterface name=bond1.44 to Network name=IMI
Status: Success
Time: 2016-08-22 05:15:24,216 EDT
JobId: 1471857321329
OVM>add VlanInterface name=bond1.30 to Network name=XSI1
Command: add VlanInterface name=bond1.30 to Network name=XSI1
Status: Success
Time: 2016-08-22 05:15:39,190 EDT
JobId: 1471857337005
OVM>add VlanInterface name=bond1.31 to Network name=XSI2
Command: add VlanInterface name=bond1.31 to Network name=XSI2
Status: Success
Time: 2016-08-22 05:15:52,576 EDT
JobId: 1471857349684
```

7. In OVM-M CLI, create unclustered server pool.

> **Note**
>
> To create clustered server pool, ignore this step and proceed to next.

```
OVM>create ServerPool clusterEnable=No name=MyServerPool
description='Unclustered server pool'
```

8. In OVM-M CLI, create clustered server pool.

   This is an optional step.

   > **Note**
   >
   > Skip this step if an unclustered server pool is already created. This step is only if required to create a clustered server pool.

   a. To create a clustered server pool you must provide a file system or physical disk to use for the server pool file system. To find a file system or physical disk, use the `list` command:

```
OVM>list FileSystem
id:66a61958-e61a-44fe-b0e0-9dd64abef7e3 name:nfs on 10.172.76.125:/mnt/
vol1/poolfs03
id:0004fb0000050000b85745f78b0c4b61 name:fs on 350014ee2568cc0cf
id: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:0004fb00000500006a46a8dbd2461939 name:MyServerPool_cluster_heartbeat
id:0004fb00000500000809e28f4fab56b1 name:fs on 350014ee20137ee44
OVM>list PhysicalDisk
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
id:0004fb00001800008f6ea92426f2cfb8 name:SATA_WDC_WD5001ABYS-_WD-
WCAS86257005
```

```
id:0004fb00001800008ccb1925cdbbd181 name:SATA_WDC_WD5001ABYS-_WD-
WCAS86578538
id:0004fb0000180000e034b4662665161c name:FreeBSD (4)
```

b. Before you create a clustered server pool you must refresh the file system or physical disk to be used for the server pool file system. To refresh a file system:

```
OVM>refresh { AccessGroup | Assembly | FileServer | FileSystem |
PhysicalDisk | Repository | Server | StorageArray | VirtualAppliance }
instance
```

For example, to refresh a physical disk:

```
OVM>refresh PhysicalDisk id=0004fb000018000035ce16ee4d58dc4d
```

c. Refresh a file system:

```
OVM>refresh FileSystem name="nfs on 10.172.76.125://mnt//vol1//repo01"
OVM>create ServerPool clusterEnable=Yes filesystem="nfs on
10.172.76.125://mnt//vol1//poolfs01" name=MyServerPool
description='Clustered server pool'
```

9. In OVM-M CLI, add Oracle VM servers to the server pool.

```
OVM>add Server name=MyServer to ServerPool name=MyServerPool
```

10. In OVM-M CLI, create storage repository.

a. Find the physical disk (LUN) to use for creating the storage repository.

```
OVM>list FileServer
Command: list FileServer
Status: Success
Time: 2016-08-19 02:11:39,779 EDT
Data:
id:0004fb00000900000445dac29e88bc38  name:Local FS vms03.test.com
id:0004fb000009000045715cad6f165ecf  name:Local FS vms01.test.com
id:0004fb0000090000df4cd9c3170092e4  name:Local FS vms02.test.com
id:0004fb000009000064b96ed88a9a0185  name:Local FS vms04.test.com
```

b. Find a local file system on an Oracle VM server that has access to the LUN.

```
OVM>list FileServer
Command: list FileServer
Status: Success
Time: 2016-08-19 02:11:39,779 EDT
Data:
id:0004fb00000900000445dac29e88bc38  name:Local FS vms03.test.com
id:0004fb000009000045715cad6f165ecf  name:Local FS vms01.test.com
id:0004fb0000090000df4cd9c3170092e4  name:Local FS vms02.test.com
id:0004fb000009000064b96ed88a9a0185  name:Local FS vms04.test.com
```

c. Create file system.

```
OVM>create FileSystem name=VmsFs01
physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e490ac3f392" on
FileServer name="Local FS vms01.test.com"
```

Command:

```
create FileSystem name=VmsFs01
physicalDisk="OVM_SYS_REPO_PART_3600605b00a2a024000163e490ac3f392" on
FileServer name="Local FS vms01.test.com"
Status: Success
Time: 2016-08-19 02:22:46,581 EDT
JobId: 1471587738752
Data:
id:0004fb00000500006779d42da60c0be6 name:VmsFs01
```

d. Create repository.

```
OVM>create Repository name=Vms01Repo on FileSystem name=VmsFs01
```

Command:

```
create Repository name=Vms01Repo on FileSystem name=VmsFs01
Status: Success
Time: 2016-08-19 02:24:04,092 EDT
JobId: 1471587843432Data:id:0004fb00000300003c8f771791114d53
name:Vms01Repo
```

e. Add server pool to repository.

```
OVM> add ServerPool name=TestPool001 to Repository name=Vms01Repo
```

Refresh the storage repository using the syntax:

```
OVM> refresh Repository name=MyRepository
```

D.2 Server Pool

A server pool is a required entity in Oracle VM, even if it contains a single Oracle VM Server. In practice, several Oracle VM servers form a server pool, and an Oracle VM environment may contain one or several server pools. Server pools are typically clustered, although an unclustered server pool is also possible. Server pools have shared access to storage repositories and exchange and store vital cluster information in the server pool file system. Refer to *Oracle VM Concepts Guide* for more information.

E

Scale a Signaling Node

Perform this procedure only if an additional signaling node(s) needs to be deployed to an existing DSR deployment.

> **Note**
>
> This procedure is only required if additional Signaling Node(s) needs to be deployed to an existing DSR deployment.

Prerequisites:

DSR topology is already deployed and configured as per Software Installation Using HEAT Templates (OpenStack).

1. Create new signaling stack.
   a. Prepare OpenStack templates and environment files for signaling stacksby following instructions in **<Procedure 13>** for signaling stacks.
   b. Create OpenStack parameter file for signaling stacks by following instructions in **<Procedure 15>**.

      > **Note**
      >
      > Change the number of signaling node(s) as per the requirement.

   c. Deploy the stacks by following instructions in **<Procedure 16>**.

      > **Note**
      >
      > New stack is created as part of this procedure.

2. Configure new site in the existing topology.
   - Create a new network element by following **<Procedure 25>** to define the network for new site being configured.
   - Configure the SOAM servers by following **Procedure 26** to create the SOAM servers.
   - Configure the SOAM server group by following **Procedure 27** to create SOAM server group.
   - Configure the MP virtual machines by following **Procedure 28**.
   - Configure the MP server group(s) and profiles by following **Procedure 31**.
   - Configure the signaling network routes by following **Procedure 32**.
   - If deployed stack contains IPFE servers, then configure the IPFE by following **Procedure 34**.

ⓘ **Note**

Repeat this procedure if more signaling nodes are required.

F

Firewall Ports

Table F-1 Firewall Ports

Flow Description	Purpose	Protocol/Port	IP Protocol Version
NTP flow for time sync	XMI network	UDP:123	IPv4, IPv6
hostname resolution (dns)	XMI, IMI Network	UDP/TCP: 53	IPv4, IPv6
LightWeight Directory Access Protocol (LDAP)	XMI network	UDP/TCP: 389	IPv4, IPv6
SSH	XMI network	TCP: 22	IPv4, IPv6
GUI	XMI network	TCP: 80, TCP:443	IPv4, IPv6

For information about Firewall Ports, refer to *DSR IP flow document*.

G

Application VIP Failover Options (OpenStack)

G.1 Application VIP Failover Options

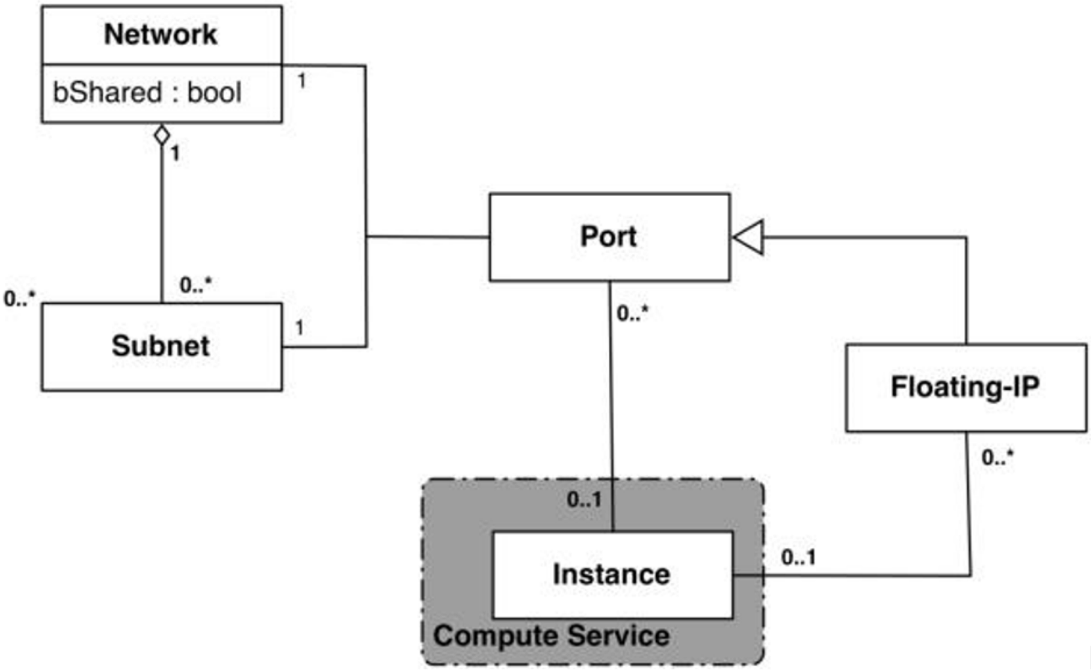
Within an OpenStack cloud environment, there are several options for allowing applications to manage their own virtual IP (VIP) addresses as is traditionally done in telecommunications applications. This document describes two of those options:

- 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 below figure.

Figure G-1 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
- 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 using 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 use 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, that is, 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 run 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 bolded items have the following meaning:

- <Port ID>
  Identifies the ID of the port within Neutron which can be determined by listing the ports, `neutron port-list`, or if the port is named then the port ID can be obtained directly in the above command with a sequence like `$ (neutron port-show –f value –F id <Port Name>)` to replace the <Port ID> placeholder.
- <VIP address to be added>

Identifies the IP address, a virtual IP address in this case, that should additionally be associated with the port where this can be a single IP address, for example, 10.133.97.135/32, or a range of IP addresses as indicated by a value such as 10.133.97.128/30.

For example, if you wanted to indicate to Neutron that the allowed addresses for a port should include the range of addresses between 10.133.97.136 to 10.133.97.139 and the port had an ID of 8a440d3f-4e5c-4ba2-9e5e-7fc942111277, then you would type the following command:

```
# 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 bolded items have the following meaning:

- <Port Name>
  This is effectively a string alias for the port that is useful when trying to locate the ID for the port but the **–-name <Port Name>** portion of the command is completely optional.
- <Subnet name>
  The name of the subnet to which the port should be added.
- <Target IP address>
  The unique IP address to be associated with the port.
- <Network Name>
  The name of the network with which the port should be associated.
- <VIP address to be added>
  This parameter value has the same meaning as described in the previous section.

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, to disable the Neutron anti-spoofing filter rules for a given port. This option allows all IP packets originating from the VM instance to be propagated no matter whether the source IP address in the packet matches the IP address associated with the Neutron port or not. This option relies upon the Neutron port security extension that is available starting with the OpenStack Kilo release.

The three sub-sections that follow describe the OpenStack configuration requirements for this option, how to use this option after a VM instance has already booted, and how to 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 the 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, and so on, 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
- Recreate the previously defined Neutron resources (networks, subnets, ports, and so on)
- 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 run 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 bolded item has the following meaning:

- <VM instance name>
  Identifies the name of the VM instance for which the identified security group name should be deleted.
- <Security group name>
  Identifies the name of the security group that should be removed from the VM instance.

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 bolded item has the following meaning:

- <Port ID>
  Identifies the ID of the port within Neutron which can be determined by listing the ports, `neutron port-list`, or if the port is named then the port ID can be obtained directly in the above command with a sequence such as `$(neutron port-show –f value –F id <Port Name>)`.

So for example if you wanted to indicate to Neutron that port security should be disabled for a port with an ID of 6d48b5f2-d185-4768-b5a4-c0d1d8075e41 then you would type the following command:

```
# 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 bolded items have the following meaning:

- <Port Name>
  This is effectively a string alias for the port that is useful when trying to locate the ID for the port but the **–-name <Port Name>** portion of the command is completely optional.
- <Subnet name>
  The name of the subnet to which the port should be added.
- <Target IP address>
  The unique IP address to be associated with the port.
- <Network Name>
  The name of the network with which the port should be associated.

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 run 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 for the way 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.

H

Sample Net Rules File

Udev uses rules files that determine how it identifies devices and creates device names. The udev daemon (udevd) reads the rules files at system startup and stores the rules in memory. If the kernel discovers a new device or an existing device goes offline, the kernel sends an event action (uevent) notification to udevd, which matches the in-memory rules against the device attributes in /sys to identify the device. As part of device event handling, rules can specify additional programs that should run to configure a device. Rules file, which have the file extension `.rules`, is located in the following directory: /etc/udev/rules.d/*.rules

Sample File:

```
# eth0 interface with MAC address "fa:16:3e:cc:12:d6" will be assigned "xmi"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="fa:16:3e:cc:12:d6", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="xmi"


# eth1 interface with MAC address "fa:16:3e:1a:8d:8a" will be assigned "int"
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="fa:16:3e:1a:8d:8a", ATTR{dev_id}=="0x0", ATTR{type}=="1",
KERNEL=="eth*", NAME="int"
```

> **Note**
>
> If you need a 3rd interface add respective entry also. The iDIH Mediation VM needs an imi interface too.

```
# 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:8a:1a:12", ATTR{dev_id}=="0x0", ATTR{type}=="1", KERNEL=="eth*",
NAME="imi":
```

> **Note**
>
> - MAC address of each interfaces can be determined using the following command issued from the console:
>
>   ```
>   ifconfig -a
>   ```
>
> - Update MAC address for each interface. The MAC addresses must be entered in all lower case.
> - Update the interface names as in the above example.

I

Performance Tuning Recommended

I.1 OpenStack

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

txqueuelen

Tuned on the compute hosts.

Purpose: The default value of 500 is too small. Our recommendation is to set to 120,000. Increases the network throughput of a VM.
On each compute host, do the following as root.

```
# cat > /etc/udev/rules.d/60-tap.rules << EOFKERNEL=="tap*", RUN+="/sbin/ip
link set %k txqueuelen 120000"EOF
```

Reload and apply to the running system.

```
# udevadm control --reload-rules
# udevadm trigger --attr-match=subsystem=net
```

Ring buffer increase on the physical ethernet interfaces

Tuned on the compute hosts.

Purpose: Improves the overall network throughput of the host.
This varies depending on the Host OS. The following steps are applicable to centos or fedora or rhel.

Add the following line into the network script of the interface you want to change.

For example: To change the ring buffer on the eth2 interface, edit `/etc/sysconfig/network-scripts/ifcfg-eth2` to add the `ETHTOOL_OPTS=` line as shown.

```
DEVICE=eth2
TYPE=Ethernet
ETHTOOL_OPTS="--set-ring eth2 rx 4096 tx 4096"
```

Restart the network using `service network restart` as root. Check the setting using `ethtool -g eth2`.

Multiqueue [on IPFE]

To be enabled on the OpenStack flavor and glance image for IPFE instance.

Purpose: Improves the network throughput of a VM.

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.

Add the following line into the network script of the interface you want to change.

For example: To set the number of queues to number of vcpus.

Edit `/etc/sysconfig/network-scripts/ifcfg-eth_interface` to set the multiqueue value to the number of vCPUs:

```
DEVICE=eth
TYPE=Ethernet
ETHTOOL_OPTS="-L ${DEVICE} combined <no_of_vCPUs>
```

Restart the network using `service network restart` as `root`.

Check the setting using `ethtool -l <eth_interface>`.

I.2 VMware

txqueuelen

Tuned on the ESXi hosts.

Purpose: Default value of 500 is too small. The recommendation is to set to 10000 which increases the network throughput of a VM.ESXi defaults the value to 500 and permits a max value of 10000.

Log in to the CLI console of the ESX host and run the below esxcli command:

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

Increase Ring Buffer on the Physical Ethernet interfaces

Tuned on the ESXi hosts.

Purpose: Improves the overall network throughput of the host. On an ESXi host Rx buffer defaults to 512 and Tx buffer defaults to 1024 and the max value for both is 4096.

Log in to the CLi console of the ESX host and run the below esxcli commands:

```
# esxcfg-nics -l (lists all the physical NICs attached to the host)
# ethtool -g <interface name> (shows the current ring buffer size)
# ethtool -G <interface name> rx 4096  (increases the rx buffer size to 4096)
# ethtool -G <interface name> tx 4096  (increases the tx buffer size to 4096)
```

Multiqueue

Already enabled on ESXi for vmxnet3 adapters.

Purpose: Improves the network throughput of a VM.

Advanced NUMA settings

Tuned on ESXi hosts.

Purpose: Prevents the ESXi scheduler to move VMs around from one NUMA node to another.

Log in to the CLI console of the ESX host and run the below esxcli commands:

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

I.3 Multiqueue on IPFE (KVM)

To enable multique on the KVM flavor and glance image for the IPFE instance. Perform the following procedure, this improves the network throughout VM.

Update the flavor and image to enable multiqueue. All guests using that image are created with multiqueue enabled. By default, the combined number of queues for a VM is 1. KVM supports a maximum of 8 queues per VM in its TAP devices.

> ⓘ **Note**
>
> The maximum number of queues can be increased in the VM's configuration XML, but it must also be set within the VM during runtime.

1. Enable Multiqueue on IPFE:

   Increase the number of queues. By default, the combined number of queues for a VM is 1. KVM supports a maximum of 8 queues per VM in its TAP devices.
   The KVM only supports a maximum of eight queues per VM in its TAP devices.

   > ⓘ **Note**
   >
   > The max can be increased in the VM's configuration XML but must be set to max inside the VM during runtime.

2. View the list of all the VMs:

   ```
   # virsh list --all
   ```

3. Shut down the VM before modifying its XML configuration:

   ```
   virsh shutdown <VM Name>
   ```

4. Edit the VM's XML configuration to set the maximum number of combined RX and TX queues:

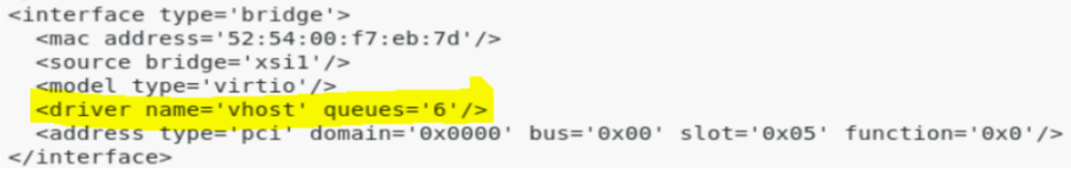
   ```
   # virsh edit <VM Name>
   ```

   Example: `virsh edit DSRMP`

5. Locate the XML tag for `<interface ..>` and modify it for each interface.

   > **Note**
   >
   > Follow this process for all the interfaces in the XML.

   The existing interface tag appears as below:

   ```
   <interface type='bridge'>
     <mac address='52:54:00:f7:eb:7d'/>
     <source bridge='xsi1'/>
     <model type='virtio'/>
     <driver name='vhost' queues='6'/>
     <address type='pci' domain='0x0000' bus='0x00' slot='0x05' function='0x0'/>
   </interface>
   ```

6. Modify the XML and add the following line to the interface.

   ```
   <driver name='vhost' queues='6'/>
   ```

   Here, 6 represents the number of queues and can be maximum upto 8.

   The updated tag appears as below:

   ```
   <interface type='bridge'>
       <mac address='52:54:00:bf:2f:a0'/>
       <source bridge='xsi1'/>
       <model type='virtio'/>
       <driver name='vhost' queues='6'/>
       <address type='pci' domain='0x0000' bus='0x00' slot='0x05'
   function='0x0'/>
   </interface>
   ```

7. After the XML is modified, Perform the following command to start the VM for the changes to take effect:

   ```
   virsh start <VM Name>
   ```

8. Log in to the VM using the IP or virsh console and set the number of multiqueues as required for the interfaces.

   ```
   # virsh console <VM Name>
   ```

9. Run the following command to make these changes persistent. To change `ethx` interface, edit `/etc/sysconfig/network-scripts/ifcfg-ethx` file and edit or append "ethx combined" in this parameter `ETHTOOL_OPTS=` as shown below.

   ```
   ETHTOOL_OPTS="......;--set-channels ethx combined 6"
   ```

> **Note**
>
> The value 6 is for number of `vcpu` in the VM. Modify the value according to your VM.

10. Set the number of combined queues to 6:

    ```
    # ethtool -L eth2 combined 6
    ```

    > **Note**
    >
    > Perform this for all the interfaces (xsi1 and xsi2). The number of combined queues can vary from 1 to the value set in the guest XML in Step 5.

11. To verify, list the current number of combined queues for the interface:

    ```
    [root@DSR-Gen10-ol7 administrator]# ethtool -l eth2
    ```

I.4 Ring Buffer and txqueuelen Configuration (KVM) OL8.9

To enable ring buffer configuration, use the KVM flavor and glance image. This increases the network throughout the VM.

1. Ensure that the ring buffer sizes and `txqueuelen` are set to max on all the ethernet devices on the host machine.

   a. Before setting ring buffer value for VMs, verify the pre-set maximum value on the hostmachine of RX and TX for all the interfaces using the following command:

      ```
      ethtool -g <interface-name>
      ```

      For example:

      ```
      /sbin/ethtool -g eth0
      /sbin/ethtool -g eth1
      /sbin/ethtool -g eth2
      /sbin/ethtool -g eth3
      Sample output of above command:
      ethtool -g eth0
      Ring parameters for eth0:
      Pre-set maximum:
      RX: 4096
      RX Mini: n/a
      RX Jumbo: n/a
      TX: 4096
      Current hardware settings:
      RX: 2080
      RX Mini: n/a
      RX Jumbo: n/a
      TX: 2080
      ```

b. Create `30_ring_buff` file by performing the following commands:

```
[root@DSR-X9KVM-1 dispatcher.d]# cd /etc/NetworkManager/dispatcher.d/


[root@DSR-X9KVM-1 dispatcher.d]# vim 30_ring_buff
#!/bin/bash
/sbin/ethtool -G ens1f0 rx 4078 tx 4078
/sbin/ethtool -G ens1f1 rx 4078 tx 4078
/sbin/ethtool -G ens1f2 rx 4078 tx 4078
/sbin/ethtool -G ens1f3 rx 4078 tx 4078
ifconfig ens1f0 txqueuelen 120000
ifconfig ens1f1 txqueuelen 120000
ifconfig ens1f2 txqueuelen 120000
ifconfig ens1f3 txqueuelen 120000
```

> **Note**
>
> The above content is an example file, which will change according to host parameters.

c. Change the permission by performing the following command:

```
[root@DSR-X9KVM-1 dispatcher.d]# chmod +x 30_ring_buff
```

d. Use the pre-set maximum of **RX** and **TX** for each interface. Then, add the below script to file `30_ring_buff`.

```
/sbin/ethtool -G <interface-name> rx <RX-Preset Maximum> tx <TX-Preset
Maximum>
For example:
#!/bin/bash
/sbin/ethtool -G eth0 rx 4078 tx 4096
/sbin/ethtool -G eth1 rx 4078 tx 4096
/sbin/ethtool -G eth2 rx 4078 tx 4096
/sbin/ethtool -G eth3 rx 4078 tx 4096
```

> **Note**
>
> The above example files will change according to host parameters.

2. Restart all ethernet adapter eth0, eth1, eth2, and eth3 by performing the following command:

```
systemctl restart NetworkManager
```

3. Verify that the ring buffer sizes are set to max on all the ethernet devices on the host machine by performing the following command:

```
# ethtool -g <ethernet adapter>
```

Verify the same for eth0, eth1, eth2, and eth3.

4. Run the following command to verify txqueue length for the ethernet adapter to a high value on the host machine that is added on all interfaces.

   ```
   # ifconfig <ethernet adapter>
   ```

   > **Note**
   >
   > These commands were tested on OL7.7 and OL8.9 KVM host machine and might vary for different versions.

I.5 Disabling TSO GSO features for SBR server

This procedure is used to disable the TSO GSO features. This is applicable for SBR servers installed on KVM.

Run the following command to disable TSO GSO features on SBR VM:

```
ethtool -K eth<X> tso off gso off
```

After disabling the TSO GSO features, the TCP queue is cleared and replication should come up.

J

Example Files

J.1 Example Template File

Basic guidelines to follow while working with YAML files:

- The file must be ended with .yaml extension.
- YAML must be case-sensitive and indentation-sensitive.
- YAML does not support the use of tabs. Instead of tabs, it uses spaces.

YAML is a human-friendly data serialization standard for all programming languages.

The values of the **key:value** can be broadly classified into the following types:

Table J-1 key:value Types

Type	Description	Examples
string	A literal string.	“String param”
number	An integer or float.	“2”; “0.2”
comma_delimited_list	An array of literal strings that are separated by commas. The total number of strings should be one more than the total number of commas.	[“one”, “two”]; “one, two”; **Note:** “one, two” returns [“one”, ” two”]
json	A JSON-formatted map or list.	{“key”: “value”}
boolean	Boolean type value, which can be equal “t”, “true”, “on”, “y”, “yes”, or “1” for true value and “f”, “false”, “off”, “n”, “no”, or “0” for false value.	“on”; “n”

J.2 Example Parameter File

The parameter file defines the topology details. This includes all VM details such as the number of VMs, flavors, network names, etc. It is a list of key/value pairs. By referring to the parameters definition section in the template file, the initialization of the parameters has to be done in this section.

File Naming Convention

It is not mandatory to have a specific name for the file; but just to provide a self-explanatory name for the file, it is recommended to follow this convention:

`<DSR Name>_<Site Name>_<NetworkOam/SignallingNode>_Params.yaml`

Example:

- `dsrCloudInit_Site00_NetworkOam_Params.yaml`
- `dsrCloudInit_Site00_SignalingNode_Params.yaml`

Sample File

Network OAM params file

```
parameters:
    numPrimaryNoams: 1
    numNoams: 1
    noamImage: DSR-60147
    noamFlavor: dsr.noam
    primaryNoamVmNames: ["DsrSite00NOAM00"]
    noamVmNames: ["DsrSite00NOAM01"]
    noamAZ: nova
    xmiPublicNetwork: ext-net
    imiPrivateNetwork: imi
    imiPrivateSubnet: imi-sub
    imiPrivateSubnetCidr: 192.168.221.0/24
    ntpServer: 10.250.32.10
    noamSG: Site00_NOAM_SG
```

Signaling params file

```
parameters:
    numSoams: 2
    numDas: 1
    numIpfes: 1
    numStps: 0
    soamImage: DSR-60147
    soamFlavor: dsr.soam
    soamVmNames: ["DsrSite00SOAM00", "DsrSite00SOAM01"]
    daImage: DSR-60147
    daFlavor: dsr.da
    daVmNames: ["DsrSite00DAMP00", "DsrSite00DAMP01"]
    daProfileName: "VM_30K_Mps"
    ipfeImage: DSR-60147
    ipfeFlavor: dsr.ipfe
    ipfeVmNames: ["DsrSite00IPFE00", "DsrSite00IPFE01"]
    stpImage: none
    stpFlavor: none
    stpVmNames: none
    xmiPublicNetwork: ext-net
    imiPrivateNetwork: imi
    imiPrivateSubnet: imi-sub
    imiPrivateSubnetCidr: 192.167.2.0/24
    xsiPublicNetwork: ext-net
    ntpServer: 10.250.32.10
    soamAZ: nova
    daAZ: nova
    ipfeAZ: nova
    stpAZ: nova
    soamSG: Site00_SOAM_SG
    daSG: Site00_DAMP_SG
    ipfeSGs: ["Site00_IPFE_SG0", "Site00_IPFE_SG1"]
    stpSG: Site00_STP_SG
    primaryNoamVmName: DsrSite00NOAM00
    noamXmiIps: ["10.75.191.170"]
    diameterTcpPorts: [3868]
    diameterSctpPorts: []
    stpSctpPorts:[]
```

Network OAM params file (Fixed IP)

```
parameters:
    numPrimaryNoams: 1
    numNoams: 1
    noamImage: DSR-8.2.0.0.0_82.5.1.vmdk
    noamFlavor: dsr.noam
    primaryNoamVmNames: ["DsrSite00NOAM00"]
    noamVmNames: ["DsrSite00NOAM01"]
    noamAZ: nova
    primaryNoamXmiIps: ["10.196.12.83"]
    noamXmiIps: ["10.196.12.84"]
    noamVip: 10.196.12.85
    xmiPublicNetwork: ext-net3
    imiPrivateNetwork: imi
    imiPrivateSubnet: imi-sub
    imiPrivateSubnetCidr: 192.168.221.0/24
    ntpServer: 10.75.185.194
    noamSG: Site00_NOAM_SG
```

Signaling params file (Fixed IP)

```
parameters:
    numSoams: 2
    numDas: 2
    numIpfes: 1
    numStps: 0
    soamImage: DSR-8.2.0.0.0_82.5.1.vmdk
    soamFlavor: dsr.soam
    soamVmNames: ["DsrSite00SOAM00", "DsrSite00SOAM01"]
    soamXmiIps: ["10.196.12.83", "10.196.12.84"]
    soamVip: 10.196.12.86
    daProfileName: "VM_30K_Mps"
    daImage: DSR-8.2.0.0.0_82.5.1.vmdk
    daFlavor: dsr.da
    daVmNames: ["DsrSite00DAMP00", "DsrSite00DAMP01"]
    daMpXmiIps: ["10.196.12.25", "10.196.12.26"]
    daMpXsiIps: ["10.196.52.73", "10.196.52.74"]
    ipfeImage: DSR-8.2.0.0.0_82.5.1.vmdk
    ipfeFlavor: dsr.ipfe
    ipfeVmNames: ["DsrSite00IPFE00", "DsrSite00IPFE01"]
    ipfeXmiIps: ["10.196.12.85"]
    ipfeXsiIps: ["10.196.52.75"]
    ipfeXsiPublicIp: 10.196.52.80
    stpImage: DSR-8.2.0.0.0_82.5.1.vmdk
    stpFlavor: dsr.vstp
    stpVmNames: ["DsrSite00STP00", "DsrSite00STP01"]
    stpXmiIps: ["10.196.12.29", "10.196.12.30"]
    stpXsiIps: ["10.196.52.77", "10.196.52.78"]
    xmiPublicNetwork: ext-net3
    imiPrivateNetwork: imi
```

```
imiPrivateSubnet: imi-sub
imiPrivateSubnetCidr: 192.167.2.0/24
xsiPublicNetwork: ext-net2
ntpServer: 10.250.32.10
soamAZ: nova
daAZ: nova
ipfeAZ: nova
stpAZ: nova
soamSG: Site00_SOAM_SG
daSG: Site00_DAMP_SG
ipfeSGs: ["Site00_IPFE_SG0", "Site00_IPFE_SG1"]
stpSG: Site00_STP_SG
diameterTcpPorts: [3868]
diameterSctpPorts: []
stpSctpPorts:[]
```

Glossary

Index