Deploying Oracle Communications Operations Monitor (OCOM) in VMware TCI 2.2 Cloud Director Edition

Technical Application Note

ORACLE
COMMUNICATIONS

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Revision History

Version	**Description of Changes**	**Date Revision Completed**
1.0	Deploying Oracle Communications Operations Monitor (OCOM) in VMware TCI 2.2 Cloud Director Edition	03rd November 2023

Table of Contents

1. Intended Audience

This document is intended for use by Oracle Systems Engineers, third party Systems Integrators, Oracle customers and partners and end users of the Oracle Communications Operations Monitor (OCOM). It is assumed that the reader is familiar with basic operations of the Oracle Communications Operations Monitor platform along with VMware TCI 2.2. Cloud Director Edition.

2. Document Overview

This Oracle technical application note outlines how to configure the Oracle Communications Operations Monitor in the VMware TCI 2.2 cloud Director Infrastructure. In this app note document, we deploy the Oracle Communications Operations Monitor hereafter referred as OCOM in standalone mode as an example. To install OCOM, the pre-requisite is that we need to install Oracle Linux OS after which we will be installing the OCOM over Linux OS. The solution contained within this document has been tested using Oracle Communication Operations Monitor with software version **OS5.0 (5.0.0.5.0)**

Please find the related documentation links below:

- Oracle Communications Operations Monitor Installation Guide
- Oracle Communications Operations Monitor User Guide
- Oracle Communications Operations Monitor Release Notes

Please note that the IP Addresses, FQDN and configuration names and details given in this document are used for reference purposes only. These same details cannot be used in customer configurations. End users of this document can use the configuration details according to their network requirements. There are some public facing IPs (externally routable IPs) that we use for our testing are masked in this document for security reasons.
The customers can configure any publicly routable IPs for these sections as per their network architecture needs.

3. Requirements

3.1. Profile to be used in Vmware TCI 2.2 Director:

VNF Component(s)	Resource allocation	Reservations
OCOM	• vCPUs: 8, vRAM: 8 GB • vDisks: Disk#1 220 GB • vNICs (VMXNET3): ○ vNIC#1 (MGMT) ○ vNIC#3 (Media)	• Total CPU Reservation • Total Memory Reservation

3.2. VMware Ready for Telco Cloud Infrastructure 2.2

Oracle Communications Operations Monitor was certified with the following components from VMware Ready for Telco Cloud Infrastructure 2.2 Cloud Director Edition Platform:

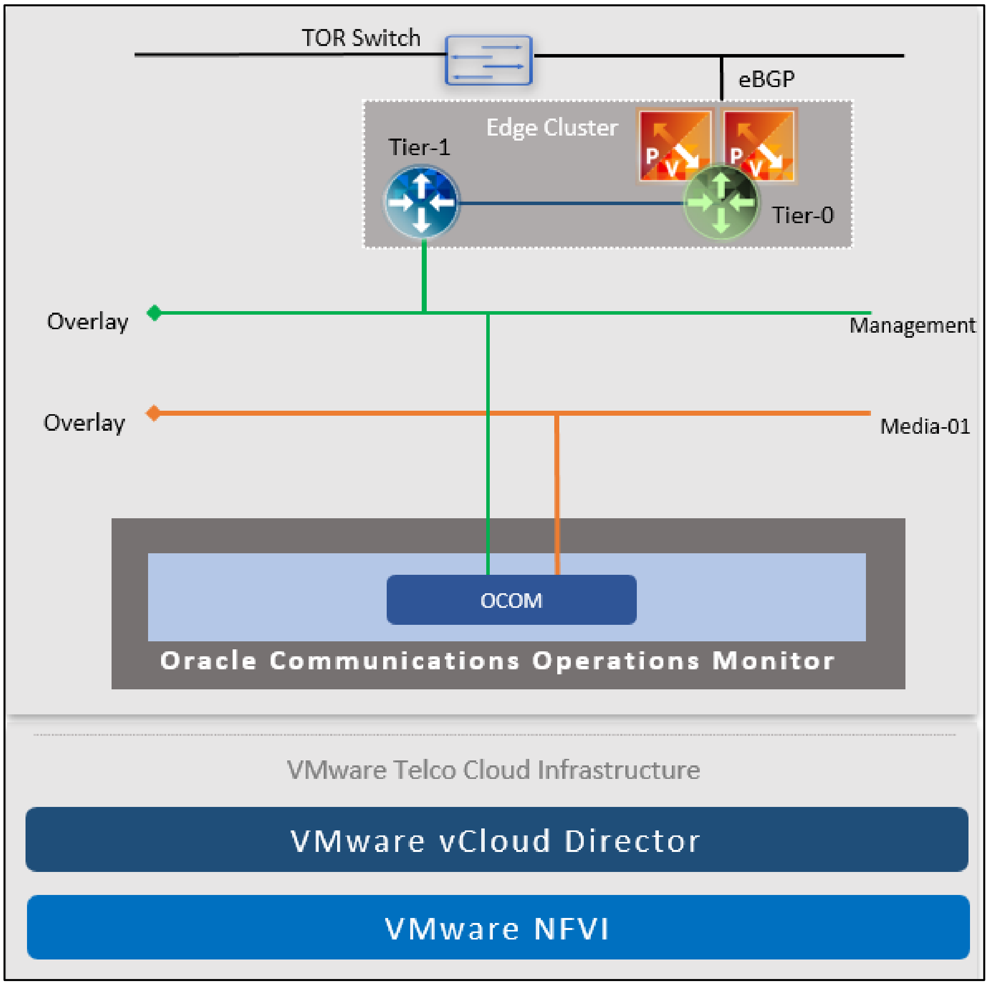
- VMware ESXi 7.0 U3c
- VMware vCenter Server Appliance 7.0 U3c
- VMware Virtual SAN 7.0 U3c
- VMware NSX-T 3.2.0.1
- VMware vCloud Director for Service Providers 10.3.2a
- VMware vRealize Log Insight 8.6.2

The below revision table explains the versions of the software used for each component:
This table is Revision 1 as of now:

Software Used	OCOM Version
Revision 1	5.0.0

3.3. Network Architecture

Below is the network architecture for the deployment of the OCOM in the VMware cloud infrastructure.



4. Create and Deploy on VMware TCI 2.2 Cloud Director

4.1. Prerequisites

- Oracle recommends the virtual datacenter used for the deployment of Communications Operations Monitor must have the allocation model as Reservation.
- The assumption here is that vCloud Director Provider VDC, Organization and Organization VDC should be available and configured in vCloud environment.
- Organization should have the below network available.
  NSX-T backed imported OrgVDC Networks (Standard Overlay, Standard VLAN, Enhanced Overlay) must be available as per VNF requirement.
- For more details on VCD specifics, refer to VMware vCloud Director user guide.

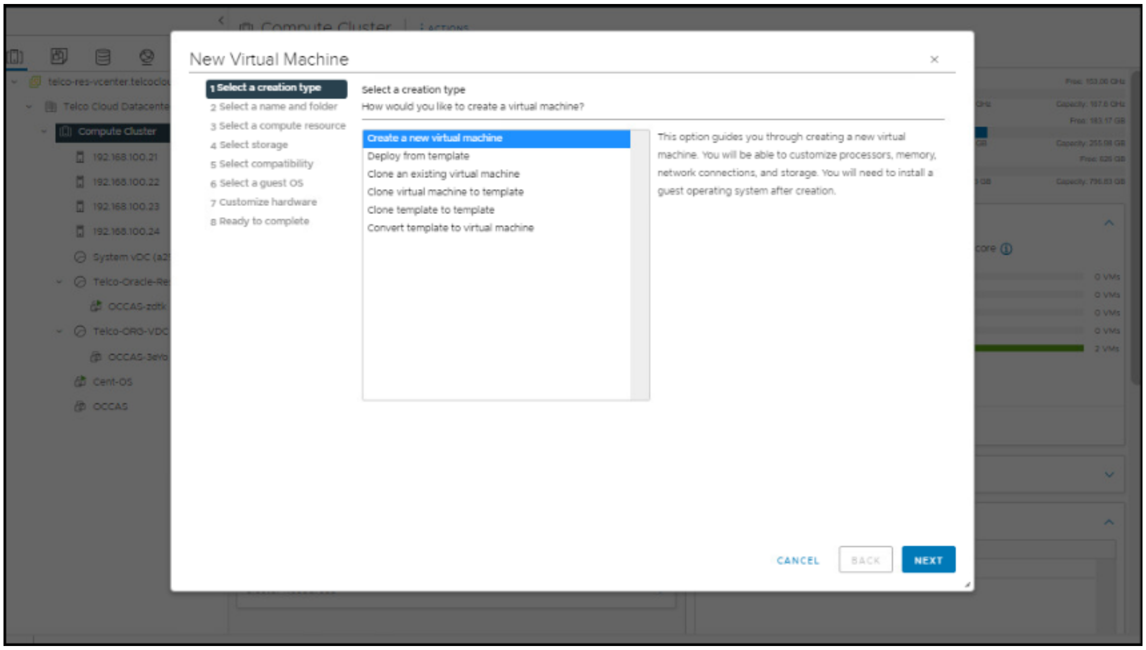
4.2. Linux OS installation

We need to install Linux OS on the VMware instance as a pre-requisite over which we will be installing the OCOM without which OCOM installation will not be successful. The user can install Oracle Linux 7 or 8 based on their needs. Since Oracle Linux is free to download, the user can download it and install it on the VMware cloud Director before starting the installation of the OCOM.

Please find the related documentation links below:

- https://yum.oracle.com/getting-started.html#installing-software-from-oracle-linux-yum-server
- https://yum.oracle.com/oracle-linux-isos.html#InstallationGuides
- https://edelivery.oracle.com/osdc/faces/SoftwareDelivery

The below screens explain the step-by-step procedure to create a new virtual machine in VMware cloud director which will be used to install the Oracle Linux image. Please note that we are using Oracle Linux 7.9 version in this app note document and the image should be already uploaded to the data store from where we can select the image to install the same.



New Virtual Machine

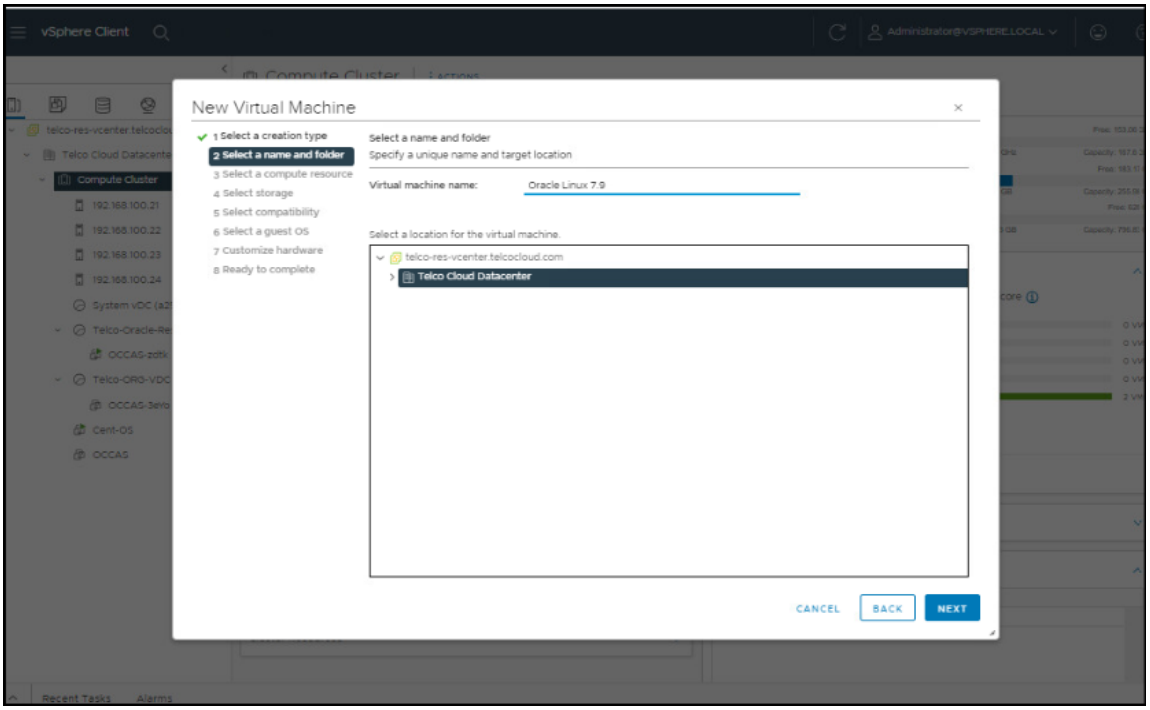
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

Select a creation type

How would you like to create a virtual machine?

- Create a new virtual machine
- Deploy from template
- Clone an existing virtual machine
- Clone virtual machine to template
- Clone template to template
- Convert template to virtual machine

This option guides you through creating a new virtual machine. You will be able to customize processors, memory, network connections, and storage. You will need to install a guest operating system after creation.



New Virtual Machine

✓ 1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

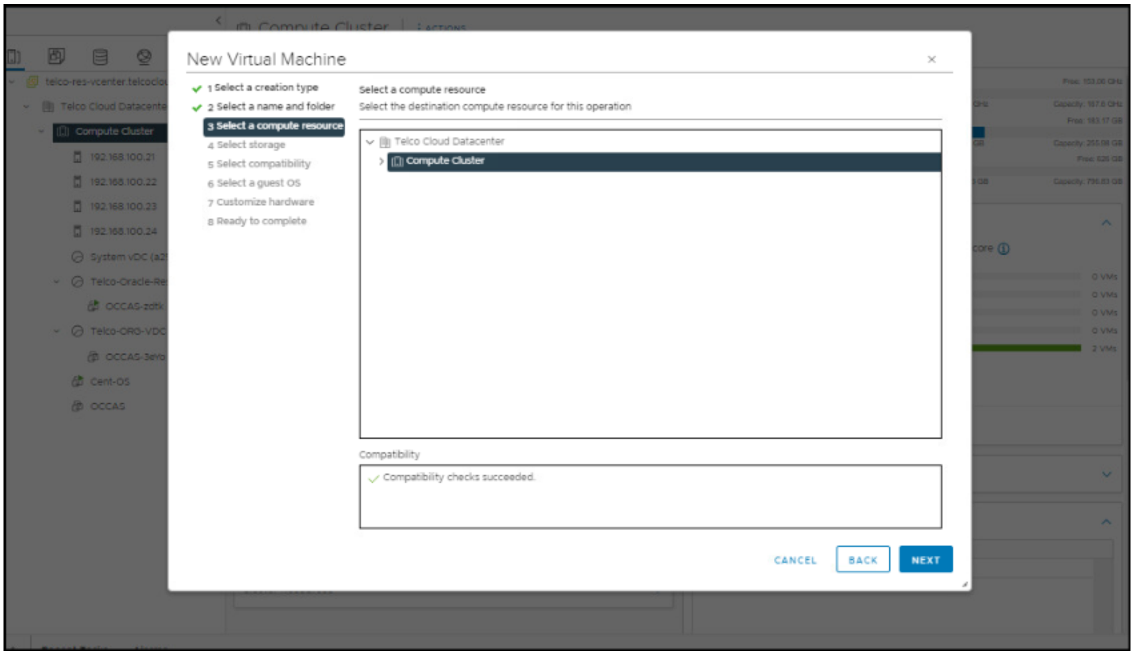
Select a name and folder

Specify a unique name and target location

Virtual machine name: Oracle Linux 7.9

Select a location for the virtual machine.

- telco-res-vcenter.telcocloud.com
  - Telco Cloud Datacenter



New Virtual Machine

✓ 1 Select a creation type
✓ 2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

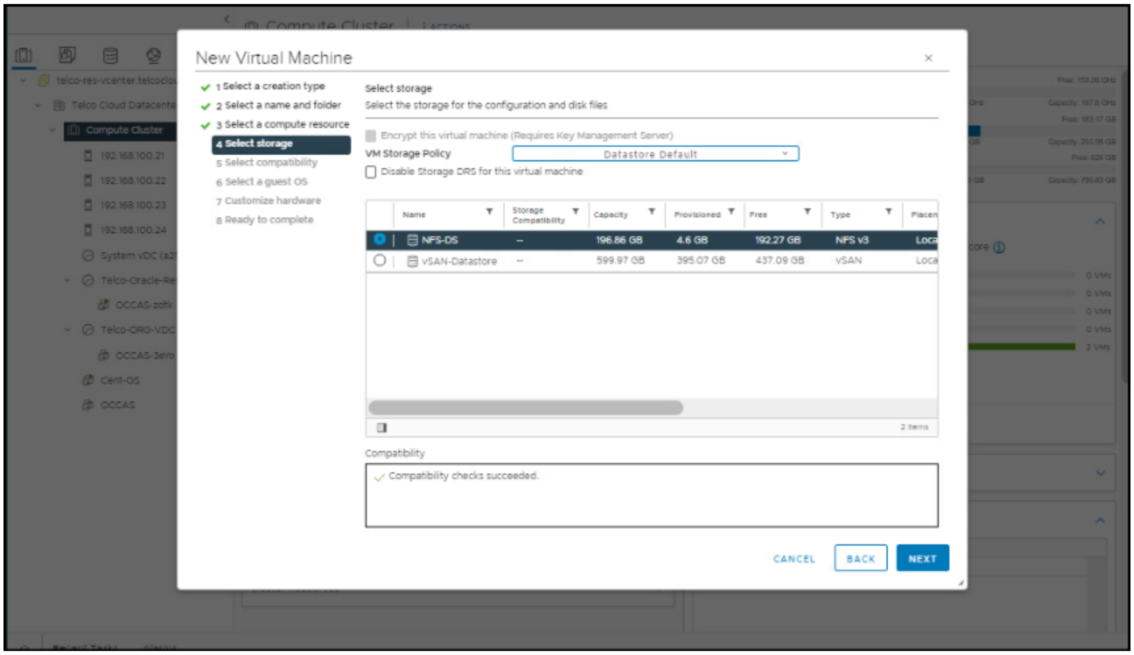
Select a compute resource

Select the destination compute resource for this operation

- Telco Cloud Datacenter
  - Compute Cluster

Compatibility

✓ Compatibility checks succeeded.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- **4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy: Datastore Default

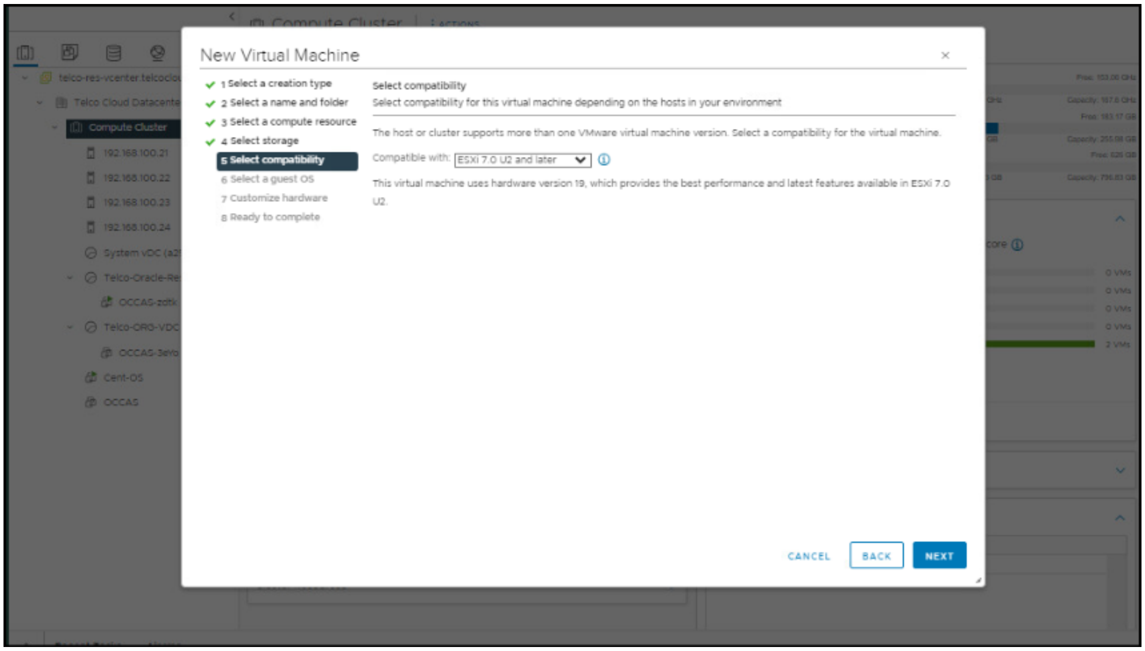
□ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Placen
●	NFS-DS	--	196.86 GB	4.6 GB	192.27 GB	NFS v3	Loca
○	vSAN-Datastore	--	599.97 GB	395.07 GB	437.09 GB	vSAN	Loca

2 items

Compatibility

✓ Compatibility checks succeeded.



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- **5 Select compatibility**
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

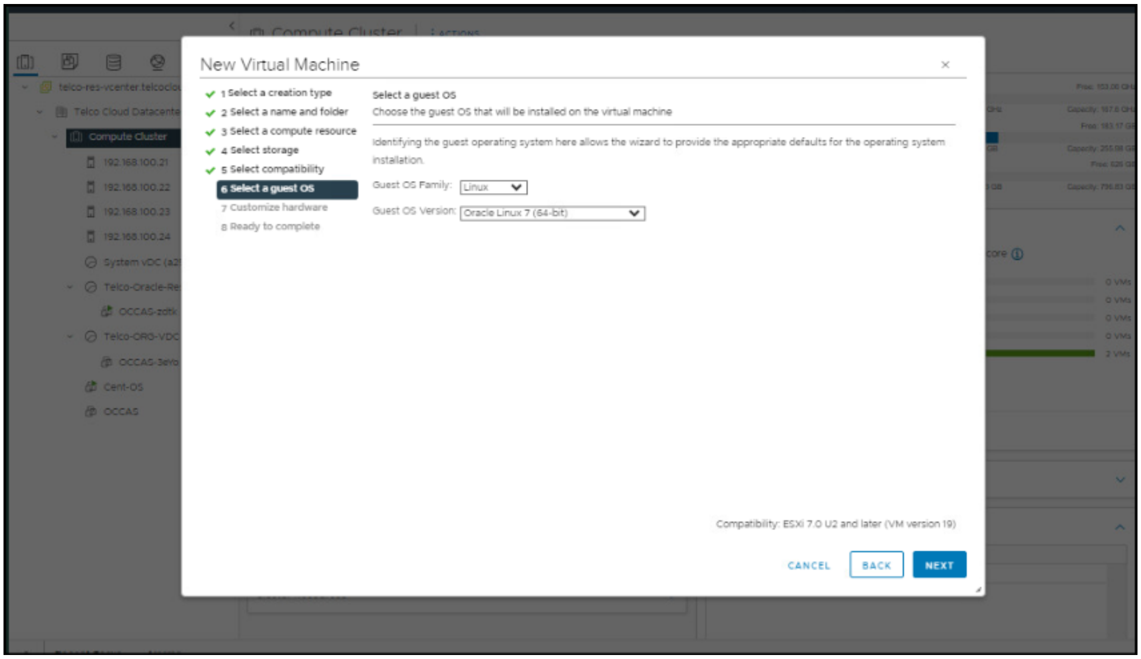
Select compatibility

Select compatibility for this virtual machine depending on the hosts in your environment

The host or cluster supports more than one VMware virtual machine version. Select a compatibility for the virtual machine.

Compatible with: ESXi 7.0 U2 and later

This virtual machine uses hardware version 19, which provides the best performance and latest features available in ESXi 7.0 U2.



New Virtual Machine

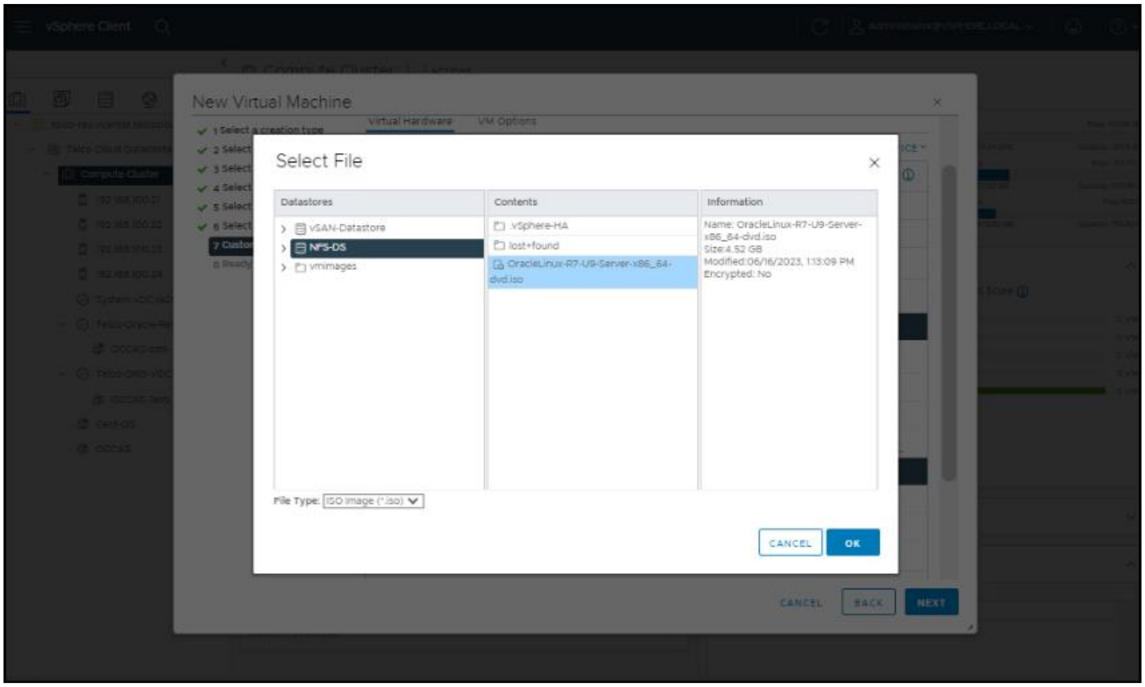
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete

Select a guest OS
Choose the guest OS that will be installed on the virtual machine

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

Guest OS Family: Linux
Guest OS Version: Oracle Linux 7 (64-bit)

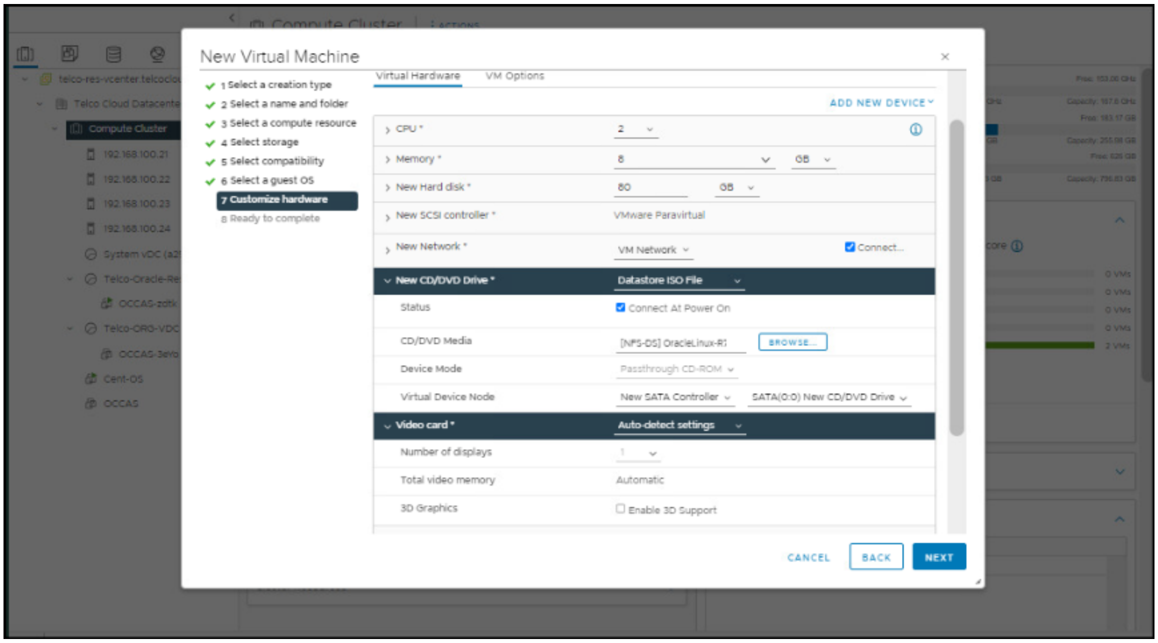
Compatibility: ESXi 7.0 U2 and later (VM version 19)



Select File

Datastores	Contents	Information
vSAN-Datastore	.vSphere-HA	Name: OracleLinux-R7-U9-Server-x86_64-dvd.iso
NFS-DS	lost+found	Size:4.52 GB
vmimages	OracleLinux-R7-U9-Server-x86_64-dvd.iso	Modified:06/16/2023, 1:13:09 PM
		Encrypted: No

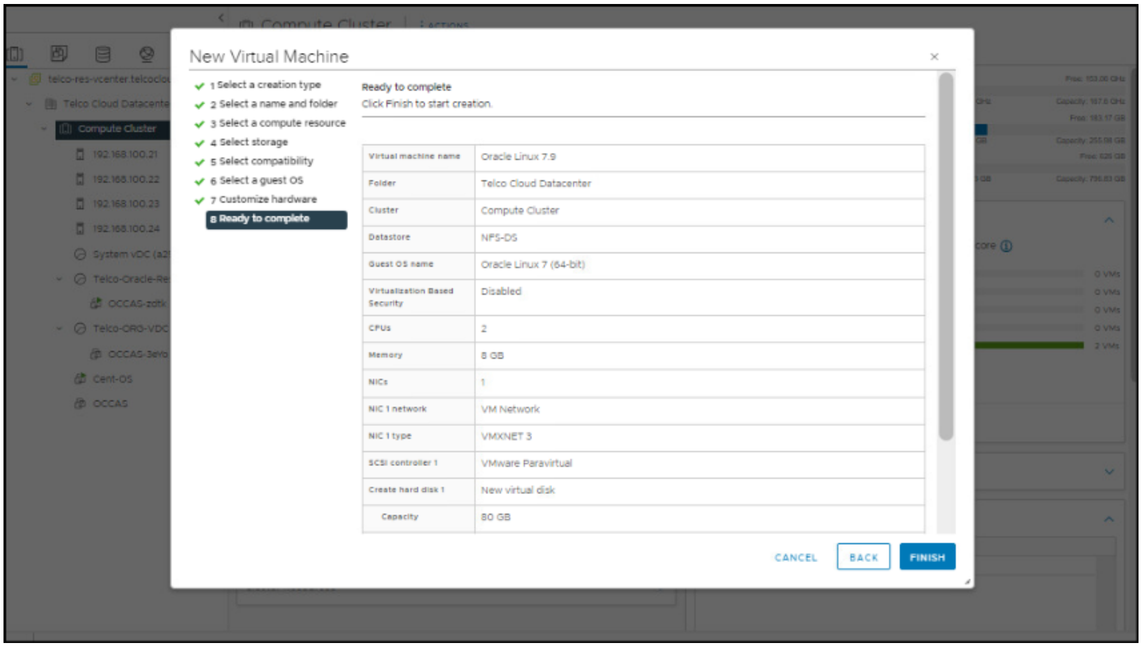
File Type: ISO image (*.iso)



New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

CPU *	2	
Memory *	8	GB
New Hard disk *	80	GB
New SCSI controller *	VMware Paravirtual	
New Network *	VM Network	☑ Connect...
New CD/DVD Drive *	Datastore ISO File	
Status	☑ Connect At Power On	
CD/DVD Media	[NFS-DS] OracleLinux-R7	
Device Mode	Passthrough CD-ROM	
Virtual Device Node	New SATA Controller	SATA(0:0) New CD/DVD Drive
Video card *	Auto-detect settings	
Number of displays	1	
Total video memory	Automatic	
3D Graphics	☐ Enable 3D Support	



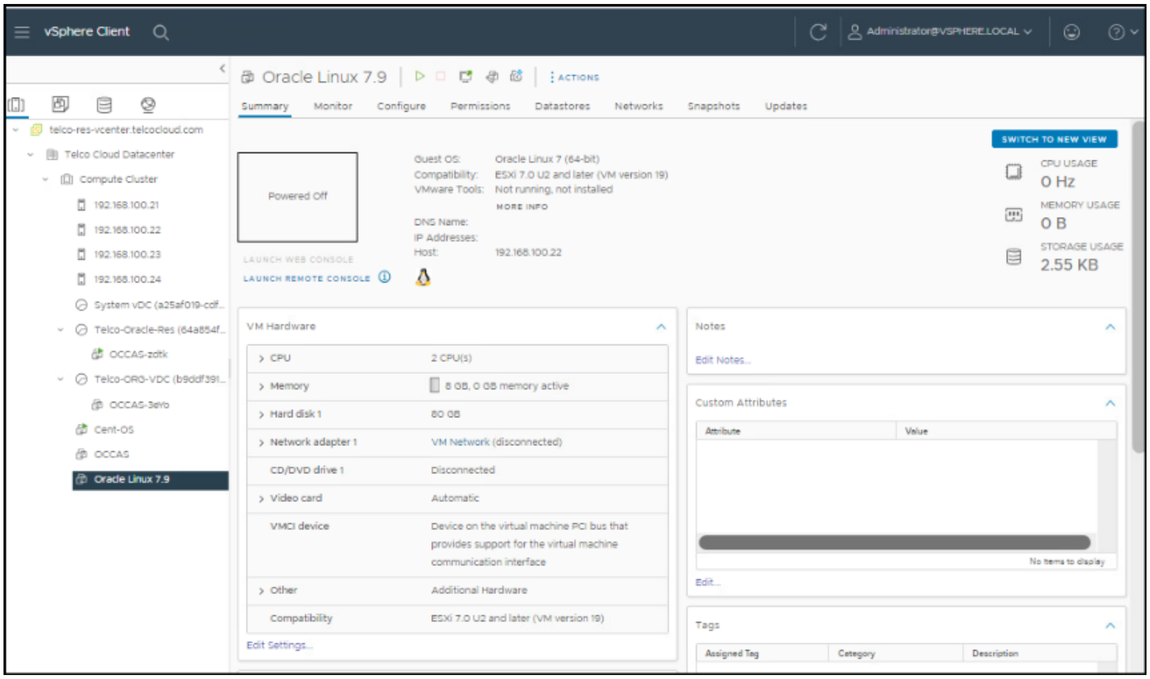
New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Select storage
- ✓ 5 Select compatibility
- ✓ 6 Select a guest OS
- ✓ 7 Customize hardware
- 8 Ready to complete

Ready to complete

Click Finish to start creation.

Virtual machine name	Oracle Linux 7.9
Folder	Telco Cloud Datacenter
Cluster	Compute Cluster
Datastore	NFS-DS
Guest OS name	Oracle Linux 7 (64-bit)
Virtualization Based Security	Disabled
CPUs	2
Memory	8 GB
NICs	1
NIC 1 network	VM Network
NIC 1 type	VMXNET 3
SCSI controller 1	VMware Paravirtual
Create hard disk 1	New virtual disk
Capacity	80 GB



Oracle Linux 7.9

Guest OS:	Oracle Linux 7 (64-bit)
Compatibility:	ESXi 7.0 U2 and later (VM version 19)
VMware Tools:	Not running, not installed
DNS Name:	
IP Addresses:	
Host:	192.168.100.22

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 2.55 KB

VM Hardware

CPU	2 CPU(s)
Memory	8 GB, 0 GB memory active
Hard disk 1	80 GB
Network adapter 1	VM Network (disconnected)
CD/DVD drive 1	Disconnected
Video card	Automatic
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other	Additional Hardware
Compatibility	ESXi 7.0 U2 and later (VM version 19)

Notes

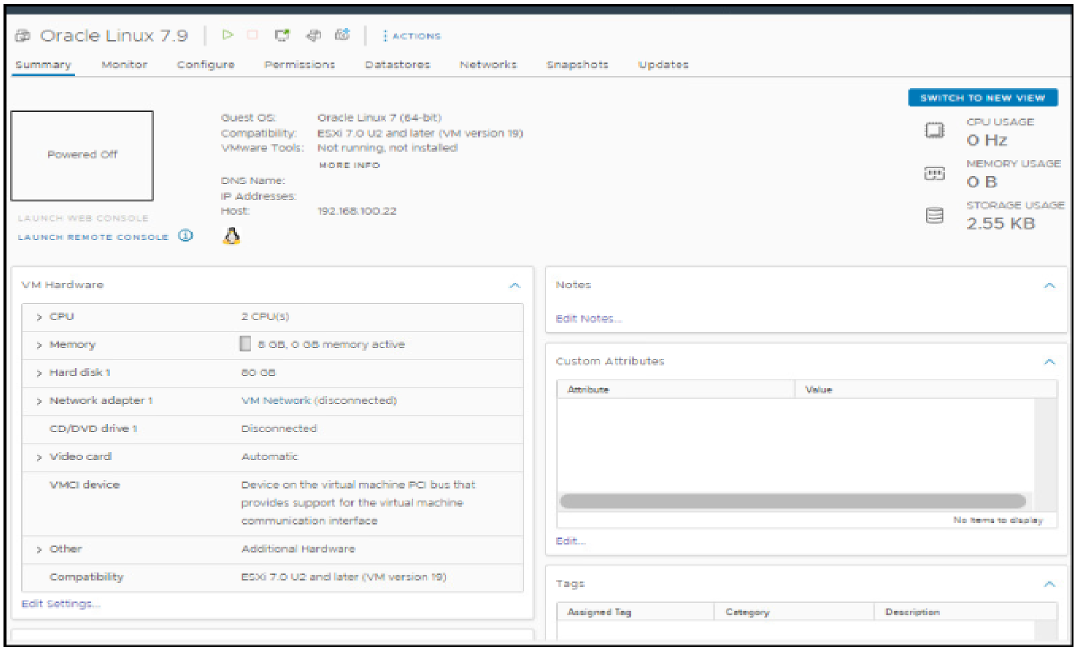
Custom Attributes

Attribute	Value

No items to display

Tags

Assigned Tag	Category	Description



Oracle Linux 7.9

Guest OS: Oracle Linux 7 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Not running, not installed
DNS Name:
IP Addresses:
Host: 192.168.100.22

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 2.55 KB

VM Hardware
CPU 2 CPU(s)
Memory 8 GB, 0 GB memory active
Hard disk 1 80 GB
Network adapter 1 VM Network (disconnected)
CD/DVD drive 1 Disconnected
Video card Automatic
VMCI device Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other Additional Hardware
Compatibility ESXi 7.0 U2 and later (VM version 19)

Notes
Custom Attributes
Attribute Value
No items to display
Tags
Assigned Tag Category Description

Please note that the installation of Linux OS is out of scope of this document as we mainly focus on OCOM deployment steps in this document.
The users can check the given link below in case they need to download and install the linux images before OCOM installation.

https://edelivery.oracle.com/osdc/faces/SoftwareDelivery

4.3. OCOM Deployment Steps on VMware

Once the Oracle Linux installation is successful as mentioned above, please start the installation of Oracle Communication Operations Monitor (OCOM) as steps given below:

1. Change the edition of MySQL to enterprise edition.
2. If you have a running Oracle Linux 7 (DPDK) probe with an Oracle Communications Session Monitor version prior to 3.4.0, uninstall Session Monitor by running the following command:

   ```
   yum remove ocsm
   ```

3. Verify that the system hosting the mediation engine is connected to the Internet.
4. Log on to the Mediation Engine server as the root user or root privileged user.
5. Verify that Oracle Linux 7 is installed by running the following command:

   ```
   cat /etc/oracle-release
   ```

6. Download the Session Monitor software by doing the following:
   a. Create a temporary directory (temp_dir) on the system that hosts the mediation engine.
   b. Download the software pack for your operating system from the Oracle software delivery web site.
   c. Download the Session Monitor installation software RPM ZIP file to temp_dir.
   d. Unzip the Session Monitor installation software RPM ZIP file.
7. Install the Session Monitor RPM file by running the following command:

   ```
   yum install ocsm-<rn>x86_64.rpm
   ```

   where:

   - <rn> is the current Session Monitor release number.
     For example, ocsm-5.0.0.0.0-397.x86_64.rpm

   The following partitioning options are available:

   - Single partition (default option)
   - Secondary partition for data storage

8. Perform the following steps to create separate partition for data (block) storage:
   a. Create the partition for data storage
   b. Run the following command to create a directory to mount the partition:

   ```
   mkdir -pv /opt/oracle/ocsm/var/vsi
   ```

   c. Adjust /etc/fstab to mount the data storage partition. For example:
   LABEL=PLD_DATA /opt/oracle/ocsm/var/vsi ext4
   defaults,nosuid,nodev,nofail 0 2
   Result: During installation partition will be detected by product setup application and the system uses the separate partition.
9. Verify the installation by doing the following:
   a. Navigate to /var/log/ocsm file.
   b. Verify whether the following log file exists: ocsm_installed_*.log
10. Adjust the firewalld to access the Session Monitor applications by doing the following:
    a. Allow firewalld to access the HTTPS service (port 443) by running the following command:

    ```
    firewall-cmd --permanent --zone=public --add-service=https
    ```

b. (Optional) If you are planning to configure the system as a mediation engine, allow the firewalld to access the probe connection by doing the following:
For SBC (embedded) probes:

```
firewall-cmd --permanent --zone=public --add-port=4739/tcp
firewall-cmd --permanent --zone=public --add-port=4740/tcp
```

For standalone probes:

```
firewall-cmd --permanent --zone=public --add-port=4741/tcp
firewall-cmd --permanent --zone=public --add-port=4742/tcp
```

c. Reload the configuration by running the following command:

```
firewall-cmd –reload
```

Enabling SELinux

Session Monitor currently supports the following top-level state of SELinux on a system – enforcing, permissive and disabled. The only supported SELinux type is targeted.

To enable SELinux:

11. Run the command to set the SELinux mode as enforcing and SELinux policy as targeted:

```
sed -i -e "s/^SELINUX=.*/SELINUX=enforcing/" /etc/selinux/config
sed -i -e "s/^SELINUXTYPE=.*/SELINUXTYPE=targeted/" etc/selinux/config
```

12. Reboot the system using the command:

```
reboot
```

13. After the reboot, run the command to verify the SELinux status:

```
Sestatus
```

Verify the command output:

```
SELinux status: enabled
SELinuxfs mount: /sys/fs/selinux
SELinux root directory: /etc/selinux
Loaded policy name: targeted
Current mode: enforcing
Mode from config file: enforcing
Policy MLS status: enabled
Policy deny_unknown status: allowed
Max kernel policy version: 31
```

14. Install the customized SELinux policy modules for Session monitor using the command:

```
cd /opt/oracle/ocsm/
./ocsm_ext.sh
```

Disabling SELinux

Use the following instructions to disable SELinux.

1. Set the SELinux mode as disabled using the command as a root user:

```
sed -i -e "s/^SELINUX=.*/SELINUX=disabled/" /etc/selinux/config
```

2. Reboot the system using the command:

```
reboot
```

3. Verify the SELinux status using the command:

```
sestatus
```

4. Verify the output:

```
SELinux status: disabled
```

Adding Ports in the SELinux Port List

On a SELinux enabled machine, in order to use any port other than the default ports in the Session Monitor, add the port in the SELinux port list using the following commands.

```
yum install -y setroubleshoot-server

semanage port -a -t <Service_Name> -p <Protocol> <Port_Number>
```

You can view all ports allowed in the SELinux using the command:

```
semanage port -l
```

For example: By default, SELinux allows http to listen on TCP ports 80, 443, 488,8008, 8009, or 8443. To configure http to run on a port other than the TCP ports listed above, such as 8001, then add the ports to the SELinux port list using the command:

```
semanage port -a -t http_port_t -p tcp 8001
```

4.4. OCOM configuration steps

1. **Configuring Proxies and Repos**

You are required to configure the proxies and repos.
Configure the http proxy in /etc/yum.conf file and also export the same to environment by doing the following.

In /etc/yum.conf, add the following line:
proxy=<Your_Proxy>
where, <your_proxy> is the proxy server details.

Run the following command to export to the environment:

```
export http_proxy=<Your_Proxy>
export https_proxy=<Your_Proxy>
```

Run the following command to enable the required proxies in yum.conf file before upgrade:

```
curl -O https://yum.oracle.com/public-yum-ol7.repo
mv public-yum-ol7.repo /etc/yum.repos.d/public-yum-ol7.repo
yum-config-manager --enable ol7_latest ol7_UEKR4 ol7_developer_EPEL
ol7_optional_
latest ol7_addons ol7_UEKR3 ol7_UEKR5 ol7_UEKR6
```

2. **Post application installation steps**.

The Platform Setup Application guides you through the Session Monitor configuration steps, including configuring the machine type, capture settings, and simple mail transfer protocol (SMTP) settings as follows:

a. Accept the license agreement to proceed with the Platform Setup Application.
b. The menu on the right shows your progress during configuration.
c. The Machine Type page sets which licensed Session Monitor applications are installed. In the Server Certificate page, you can upload your signed certificate for secure HTTPS connections.
d. Subsequent sections configure the Session Monitor server for your network. These steps are optional.
   Except for Machine Type and Extensions, you can review and change settings at any time by visiting the Platform Setup Application at https://ip_address /newsetup/, where ip_address is the IP address of the server that hosts a Session Monitor application. This URL is valid for any Session Monitor server.
e. In the final step, each selected Session Monitor application is installed.
   After a successful installation, the log in page appears for each of your licensed Session Monitor application.

3. **Platform Setup Application Initial Log In.**

All Session Monitor application interfaces are accessed through encrypted HTTPS connections. At the initial login, your web browser may not recognize the server and displays the warning:

This Connection is Untrusted. Click **Confirm Security Exception** to proceed.
For information about how to protect connections to the system and avoid the untrusted certificate warning in the future, see Oracle Communications Session Monitor Security Guide.
This section describes how to configure Session Monitor using the Platform Setup Application.

To configure Session Monitor:

a. In a web browser, go to https://<ip_address>/newsetup.
   The Platform Setup Application Login page appears.
b. In the **Username** field, enter **sysadmin** and in the **Password** field, enter **oracle**.
   The License Terms agreement page appears.
c. Accept each Session Monitor application license terms agreement, by selecting the **I agree to the license terms** check box.
d. Click **Proceed**.
   The **Change Password** dialog box appears.
   The **Platform Setup Application** page appears.
e. Change the password by doing the following:
   - In the **Set password** field, enter a **new password**.
   - In the **Repeat password** field, re-enter the password used in the previous step, which verifies that the password value was entered correctly.
   - Click **Change**.
     The **Machine Type** page appears.

4. On the Machine Type page, select the machine type on which to install your licensed Session Monitor applications and components:
   a. To install an Operations Monitor probe, select **Standalone Probe**.
   b. To choose different Session Monitor applications, select the **Mediation Engine** and then select the required product (or applications) as per the license:
      – To install Oracle Communications Operations Monitor, select the **Communications Operations Monitor** check box.
      – To install Oracle Communications Control Plane Monitor, select the **Control Plane Monitor** check box.
      – To install an Operations Monitor embedded probe, select the **Probe (embedded)** check box.
      Only the checked items are included in the installation.
5. Click Continue

   The machine type and application information appear in the status panel located on the right under the navigation list.
   The **Configuration** page appears.

6. Configure the Session Monitor settings for the machine type you chose in step 5 in accordance with the terms of your license as follows:
   a. From the Capacity section in the Concurrent calls field, enter the number of concurrent calls printed on your license.
   b. If you have licensed RTP recording, select the RTP Recording check box.
   c. From the Capacity section in the Concurrent RTP streams field, enter the number of concurrent RTP streams printed on your license.
   d. In the Additional Extensions section, select the Non Calls check box to see the Subscription panels in the user interface. You can edit this check box even after the installation is done.
   e. From the Extensions section, select all the product extensions you have licensed.
   f. Click Continue.
      The Disk Usage page appears.
   g. On the Disk Usage page, specify the maximum disk usage partition for the Packet Inspector.
7. (Optional) If you selected Probe on the Machine Type page, set which mediation engines are connected to the Operations Monitor probe.
   a. Click Add a new ME.
   b. In the Hostname or IP field, enter the IP address of the machine that hosts the mediation engine.
   c. In the Port field, enter the port number of the mediation engine. For a Cleartext transmission enter 4741 and for TLS enter 4742.
   d. In the Name field, enter a name for the mediation engine.
   e. In the TLS field, select the checkbox for TLS transmissions or leave the checkbox unchecked for Cleartext.
      The Operations Monitor Probe can transmit data to one or more mediation engines with either transport layer security (TLS) encryption, or with unencrypted Cleartext. A mediation engine can connect to more than one Operations Monitor Probe or more than one Session Border Controller Probe.
8. Click **Continue**.

   The Trusted Certificate page appears.

9. In the Upload a trusted certificate field, select Browse and locate the signed certificate file. Click Continue.

(Optional) By default, the mediation engine machine accepts only encrypted transmissions, (unless the mediation engine and probe are on the same machine); for Cleartext transmissions select the **Accept insecure connections from remote probes check box**.
Click **Continue**.
The Server Certificate page appears.

10. All Session Monitor interfaces are accessed through encrypted (secure) HTTPS connections. Each Session Monitor machine uses a unique certificate to establish secure connections and to guarantee its authenticity and protect users' data.

    Do one of the following:
    a. To use the self-signed certificate, click Continue.
    b. To sign the server certificate with your organization's Public Key Infrastructure (PKI):
        - Select **Download request**.
        - Sign the certificate with the X.509 format.
        - In the Upload signed certificate field, select Browse and locate the signed certificate file.
        - Click Continue. The SMTP Configuration page appears.

11. Session Monitor can send notifications and alerts directly to a user's email address. If you require notifications or alerts, select the Enable SMTP check box and fill in the relevant fields with your SMTP server details.

12. Click **Continue**.

    The Capture Settings page appears.

13. The Capture Settings page contains a list of configured network interfaces. Monitoring can be enabled and disabled. You should have configured network devices while installing Oracle Linux 7.

14. Click **Continue**.

    The Data Retention page appears. If you have enabled the Non Calls check box in the Configuration > Additional Extensions section, only then the Subscription Data -Subscriptions is enabled.

15. Click **Continue**.

    The Install page appears.

16. (Optional) Click Download Configuration, which downloads your configuration settings file in the default download location of your system.

17. Open the psa_conf.json configuration file and verify your settings.

18. Click **Install**.

    The Did you select the right applications dialog box appears.

19. Verify that you have chosen the correct Session Monitor applications and components for installation; after installation is complete, the selected applications and components cannot be changed.

    Click **OK**.

    The Platform Setup Application initiates the installation and reports its progress. The Installation Complete dialog box appears.

20. Do one of the following:

    - To go back to the Platform Setup Application, click **Back to Setup**.
    - To go to a Session Monitor application dashboard, **click Go to Application**.

21. The credentials for logging in to Session Monitor are:

    - For Platform Setup Application, enter the user name provided by Oracle and the password you set up in step 5.
    - For Operations Monitor and Control Plane Monitor, enter the login credentials provided by Oracle Sales Consultant.

Changing Community MySQL Edition to Enterprise Edition

Change the edition of MySQL by doing the following:

1. Go to the Oracle Software Delivery web site: https://edelivery.oracle.com
2. Read and accept the license agreement and export restrictions and click Continue.
3. Download the latest Enterprise edition of MySQL in version 5.7.38.
4. Uninstall the Community edition of MySQL by running the following command:

   ```
   yum remove -y mysql-community-common
   ```
5. List the MySQL packages that may have remained using this command:

   ```
   yum list installed mysql*
   ```
6. If you are running mysql community version 8.0, run this command to remove mysql-community-client-plug-ins.

   ```
   yum remove -y package mysql-community-client-plugins
   ```
7. Install the Enterprise edition of MySQL by running the following command:

   ```
   yum install mysql-commercial-*.x86_64.rpm
   ```
8. Install the yum utils by running the following command:

   ```
   yum -y install yum-utils
   ```
9. Enable the latest Oracle Linux 7 add-on's by running the following command:

   ```
   yum-config-manager --enable ol7_latest ol7_UEKR4 ol7_developer_EPEL l7_
   optional_latest ol7_addons ol7_UEKR3 ol7_UEKR5
   ```

4.5. Virtual Machine Probe Cloning

A cloned probe is an exact replica of the original probe having the same UUID as the original probe. However, each probe requires a unique UUID to establish a connection with the Mediation Engine. If the Probe Virtual Machine has been cloned, you must change the Unique ID of the probe after cloning and before connecting the cloned probe. Follow the instructions after cloning the probe to generate random UUID.

Ensure that the following prerequisites are taken care of:

- Cloning of the probe has been successful.
- Cloned probe is not connected to the Mediation Engine. If it was connected, remove:
  – Mediation Engine details on the probe
  – Probe details on the Mediation Engine

1. Check for the UUID of both the probes under:

   ```
   /opt/oracle/ocsm/etc/iptego/psa/probe_uuid.conf
   ```

2. Run the script to change the UUID of cloned probe:

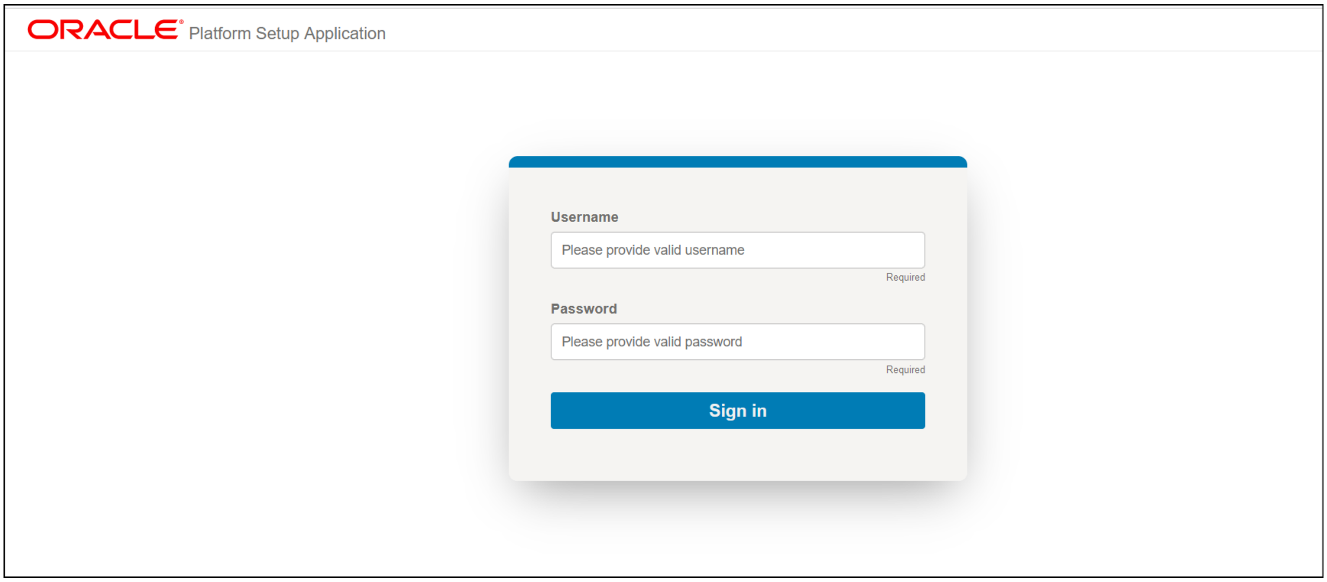
   /opt/oracle/ocsm/usr/share/pld/scripts/write_rapid_uuid.sh

3. Check the UUID and make sure that the UUID of the cloned probe has been changed after running the script in the probe_uuid.conf file

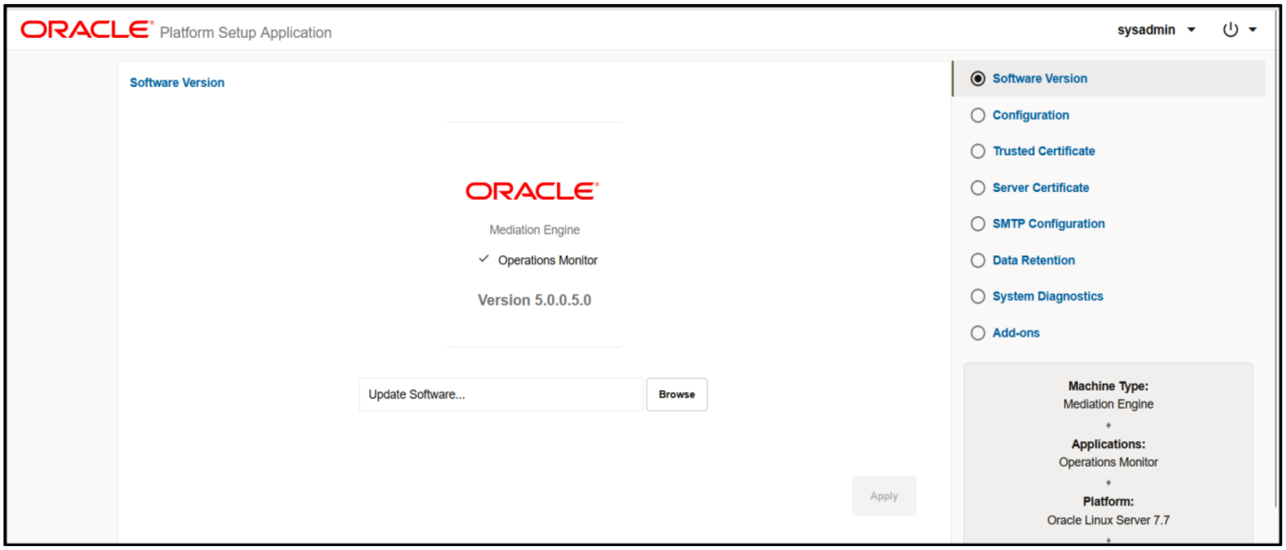
Connect the cloned probe to the Mediation Engine

5. Services Verification

Access the OCOM through URL https://<ocom-managaement-IP>/newsetup/


ORACLE Platform Setup Application
Username
Please provide valid username
Required
Password
Please provide valid password
Required
Sign in

After you enter the username and password, the OCOM GUI comes up with lot of options as seen in the right-hand side of the screen. We can select any of those options which we need to perform and can proceed accordingly.



Software Version

ORACLE

Mediation Engine

✓ Operations Monitor

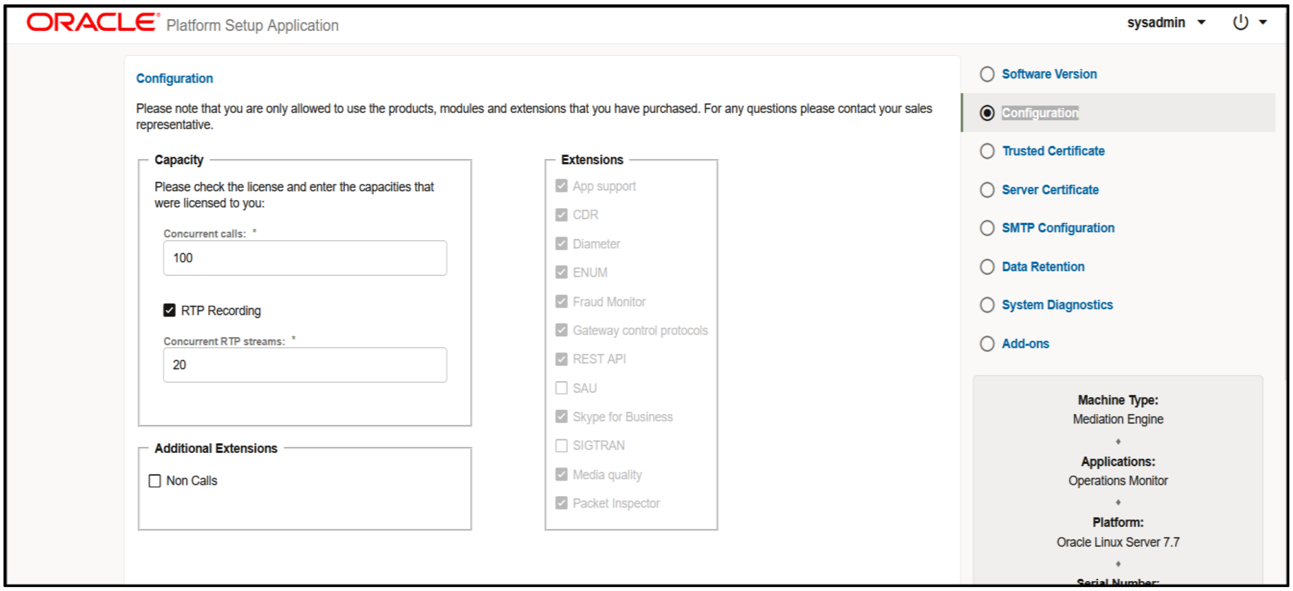
Version 5.0.0.5.0

Update Software...

Machine Type:
Mediation Engine

Applications:
Operations Monitor

Platform:
Oracle Linux Server 7.7



Configuration

Please note that you are only allowed to use the products, modules and extensions that you have purchased. For any questions please contact your sales representative.

Capacity

Please check the license and enter the capacities that were licensed to you:

Concurrent calls: * 100

☑ RTP Recording

Concurrent RTP streams: * 20

Additional Extensions

☐ Non Calls

Extensions

☑ App support
☑ CDR
☑ Diameter
☑ ENUM
☑ Fraud Monitor
☑ Gateway control protocols
☑ REST API
☐ SAU
☑ Skype for Business
☐ SIGTRAN
☑ Media quality
☑ Packet Inspector

Machine Type:
Mediation Engine

Applications:
Operations Monitor

Platform:
Oracle Linux Server 7.7

Serial Number:

For more information on OCOM, please refer the below link.

https://docs.oracle.com/en/industries/communications/session-monitor/5.0/index.html

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

- blogs.oracle.com/oracle
- facebook.com/Oracle/
- twitter.com/Oracle
- oracle.com

Integrated Cloud Applications & Platform Services