Oracle® Communications Session Monitor

Installation Guide

Release 5.1

F76419-04

October 2023

ORACLE®

Contents

3   Installing Session Monitor Offline

4   Configuring Session Monitor

5   Session Monitor Post-Installation Tasks

6 Installing and Configuring DPDK for Session Monitor

7 Downloading, Installing, and Configuring DPDK for Mellanox NIC Cards

8 Installing Skype for Business Agent

9 Public Cloud Platforms

Part I   Palladion Ports Usage

About This Guide

This guide provides instructions for installing Oracle Communications Session Monitor.

The Oracle Communications Session Monitor product family includes the following products:

- Operations Monitor
- Enterprise Operations Monitor
- Fraud Monitor
- Control Plane Monitor

Documentation Set

Table 1   Documentation Suite for OCSM 5.1

Document Name	Document Description
Backup and Restore Guide	Provides instructions for backing up and restoring Session Monitor.
Developer Guide	Contains information for using the Session Monitor SAU Extension.
Fraud Monitor User Guide	Contains information for installing and configuring Fraud Monitor to monitor calls and detect fraud.
Installation Guide	Contains information for installing Session Monitor.
Mediation Engine Connector User Guide	Contains information for configuring and using the Mediation Engine Connector.
Operations Monitor User Guide	Contains information for monitoring and troubleshooting IMS, VoLTE, and NGN networks using the Operations Monitor.
Release Notes	Contains information about the Session Monitor 5.1 release, including new features.
Security Guide	Contains information for securely configuring Session Monitor.
Upgrade Guide	Contains information for upgrading Session Monitor.

Revision History

This section provides a revision history for this document.

Date	Description
April 2023	Initial release.
May 2023	Minor updates to the content.
July 2023	Content updates for the P1 release.
October 2023	Content updates.

1

Overview of Session Monitor Installation

This chapter provides an overview of the Oracle Communications Session Monitor system architecture and the installation process.

Session Monitor System Architecture

The Session Monitor system works by capturing the traffic from your network, correlating it in real-time, and storing it in indexed formats so that they are available for the various reports offered by the web interface.

The Session Monitor system architecture has three layers:

- **Probe layer:** This layer is responsible for capturing the traffic from your network and performing the Media Quality analysis. The probes send meta-data for each of the signaling messages to the Mediation Engine layer and analyze the RTP streams locally, sending the results of this analysis to the Mediation Engine layer.

- **Mediation Engine (ME) layer:** This layer is responsible for understanding in real-time the traffic received, correlating it and storing it for future reference. This layer is also responsible for measuring, managing, and storing the KPIs. In the common case, there is one ME per geographical site. It is possible, however, to have the probes from multiple geographical sites sending the traffic to a single ME. It is also possible to have multiple ME installations in the same geographical site.

- **Aggregation Engine (AE) layer:** This layer is responsible for aggregating the global KPIs from all the MEs linked to it, and for the global search features. In a typical setup, there is only one AE for the whole network.
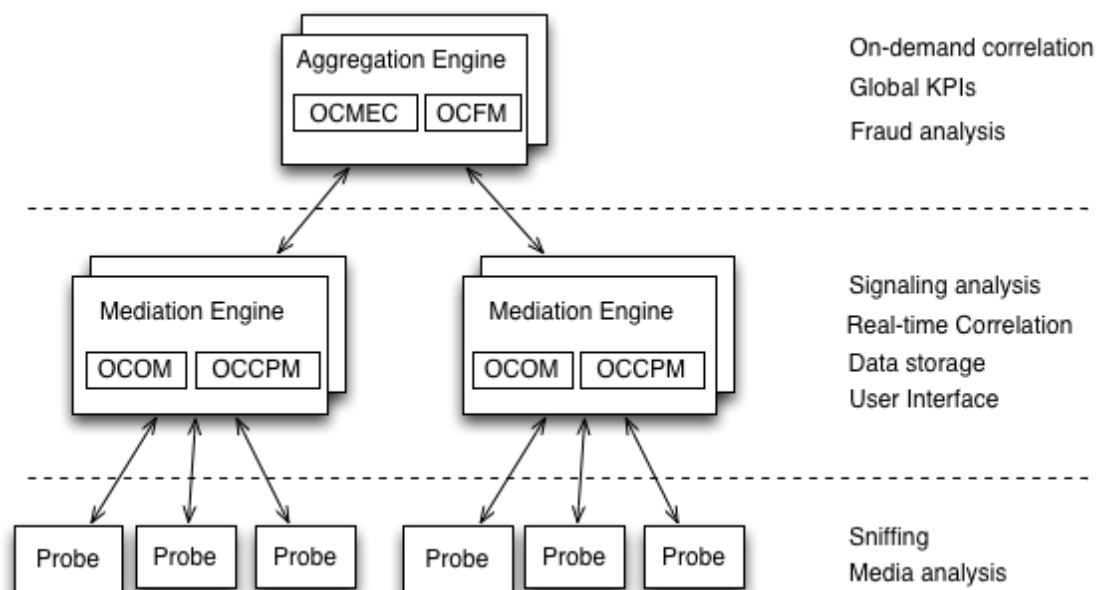
Each of the three layers supports high-availability by deploying two identical servers in active-passive or active-active modes of operation. For small setups, it is possible to run the probe layer and the ME layer on the same physical hardware. The AE layer always requires its own hardware.

From the Session Monitor products perspective, the Operations Monitor and the Control Plane Monitor (CPM) run on the Mediation Engine (ME) while the Mediation Engine Connector (MEC) and the Fraud Monitor products run on the Aggregation Engine (AE).

About Installing Session Monitor

The installation of Session Monitor includes these steps:

1. Reviewing the system requirements and selecting the hardware that is needed.

2. Using the Session Monitor Installer to do the software installation.

3. Using the Platform Setup Application for initial system configuration.

Session Monitor System Requirements

Before installing Session Monitor using the .rpm file, ensure that partitions and disk size for the data (block) storage and MySQL storage are as per the desired retention period. It is recommended to complete a sizing exercise with assistance from your Oracle sales engineer.

Session Monitor System Requirements are found in the Release Notes.

Network Monitoring Modes

Session Monitor probes can use two modes of monitoring network mode:

- **mmpcap:** The **mmpcap** mode is based on the **libpcap** Packet Capture Library similar to **tcpdump**, using the Kernel's Packet Socket Interface. The network interface is set to promiscuous mode.

- **Data Plane Development Kit (DPDK):** DPDK is a set of data plane libraries and network interface controller drivers for fast packet processing. In this mode, the network interface is no longer accessible by the Kernel. You can find more information regarding the DPDK libraries in the website, http://dpdk.org.

By default, the installer enables the **mmpcap** mode which is recommended for small to medium installations (for up to 1400K pps depending on server capabilities). For higher network traffic solutions, you may choose to enable **DPDK** mode for better performance. For more information on DPDK, see Installing and Configuring DPDK for Session Monitor.

> ✎ **Note:**
>
> The above number is only for reference. The actual decision on when to use DPDK depends on many factors. For consulting regarding this decision, Oracle recommends to complete a sizing exercise together with your Oracle sales engineer.

2

Installing Session Monitor

This chapter describes how to install Oracle Communications Session Monitor.

> **Note:**
>
> If you need separate partitions for data (block) storage and MySQL storage, see the section Creating a Separate Partition for Data and MySQL Storage.

Before installing Session Monitor, read the following:

- About Installing Session Monitor
- Session Monitor System Requirements

Installing Session Monitor Using the RPM

This section describes installing the Session Monitor using RPM.

You have to set up the machine with Oracle Linux 8 operating system to install Session Monitor using the RPM. Configurations are necessary for proxies and repos, if there are any, see Configuring Proxies and Repos.

To install Session Monitor using an RPM:

1. Verify that the system hosting the OCSM is connected to the Internet.

2. Log on to the OCSM server as the root user or root privileged user.

3. Run this command to verify that Oracle Linux 8 has been installed.`cat /etc/oracle-release`

4. If partitioning is required, refer to the section Creating a Separate Partition for Data and MySQL Storage.

5. Download the Session Monitor software:

    a. Create a temporary directory (temp_dir) on the system that hosts the OCSM.

    b. Download the software pack for your operating system from the Oracle software delivery website.

    c. Download the Session Monitor installation software RPM ZIP file to temp_dir.

    d. Unzip the Session Monitor installation software RPM ZIP file.

6. Download the latest MySQL 8 Commercial Package file from the Oracle software delivery website. `Patch 34982613: MySQL Database/Components 8.0.32 Yum Repository TAR for Oracle Linux / RHEL 8 x86 (64bit).`

    a. Copy the MySQL tar.gz package from the download to a temporary directory

b. Run these commands to untar the MySQL tar.gz package:

```
yum install tar
tar -xvf mysql-commercial-<rn>.x86_64.repo.tar.gz
where <rn> is the current MySQL 8 version
```

c. Move to the MySQL directory:

```
cd mysql-8.X/8.X.XX/
```

Example:

```
tar -xvf mysql-commercial-8.0.32-1.1.el8.x86_64.repo.tar.gz
cd mysql-8.0/8.0.32/
```

7. Install the MySQL 8 rpms using the command:

```
yum install mysql-commercial-*
```

Installing Python 39

Run the following commands to install Python 39 and PIP3

1. Install python39 and pip3

```
yum install python39-pip
```

2. Set Python alternatives to python3.9:

> **✎ Note:**
>
> Important! When prompted, select the number corresponding to the python3.9 option and press the Enter key.

```
update-alternatives --config python3
update-alternatives --config python
```

> **✎ Note:**
>
> After the OCSM Installation, while installing any new packages using yum, some packages will install Python 3.6 as a dependency. As a result Python alternatives will get changed. This can cause unexpected problems in the OCSM functionality. So it is mandatory for you to verify that Python is pointing to python 39 after every package installation using yum by running the above two commands.

Installing the SQL Connector

Download MySQL Connector package corresponding to the MySQL version.

1. Download MySQL Connector package corresponding to the MySQL version installed from MOS to a temporary directory of the OCSM Server, for example: If MySQL 8.0.32 Commercial is installed in the system, download the MySQL Connector 8.0.32 Package from MOS:

   ```
   (Patch 34984522: MySQL Connector/Python 8.0.32 WHL for portable Linux x86
   (64bit) Python 3.9 -- p34984522_800_Linux-x86-64.zip)
   ```

2. From the temporary directory, run the following commands to install the MySQL Connector:

   ```
   yum install unzip
   unzip pXXXXXXXX_XXX_Linux-x86-64.zip
   pip3 install mysql_connector_python-8.X.X-1commercial-cp39-cp39-
   manylinux1_x86_64.whl
   ```

   For example:

   ```
   unzip p34984522_800_Linux-x86-64.zip
   pip3 install mysql_connector_python-8.0.32-1commercial-cp39-cp39-
   manylinux1_x86_64.whl
   ```

   > ✎ **Note:**
   >
   > If required, use proxy with pip3. For example,
   >
   > ```
   > pip3 install --proxy [PROTOCOL://]HOST[:PORT]
   > mysql_connector_python-8.0.32-1commercial-cp39-cp39-
   > manylinux1_x86_64.whl
   > ```

Installing the Oracle epel Repository

Install the Oracle epel Repository:

1. Use the following commands to install the Oracle epel Repository:

   ```
   yum install oracle-epel-release-el8.x86_64
   ```

2. For OCI Cloud Machines, complete the following additional step to enable ol8_developer_EPEL repo.

   a. Using an editor, open the file `/etc/yum.repos.d/oracle-epel-ol8.repo`.

   b. Under the section [ol8_developer_EPEL] set enabled=1.

c. Save the file.

```
[ol8_developer_EPEL]
name=Oracle Linux $releasever EPEL Packages for Development
($basearch)
baseurl=https://yum$ociregion.$ocidomain/repo/OracleLinux/OL8/
developer/EPEL/$basearch/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=1
enabled=1
```

3. Install yum-utils:

   a. Use this command:

   ```
   yum install yum-utils
   ```

   b. Enable the latest Oracle Linux 8 repositories by running the following commands:

   ```
   yum-config-manager --enable
   ol8_baseos_latest ol8_appstream
   ol8_addons ol8_developer_EPEL
   ```

4. Install the Session Monitor RPM file uisng this command.

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

> **Note:**
>
> In this command, <rn> is the latest Session Monitor release number. For example, `ocsm-5.1.0.0.0-134.x86_64.rpm`.

Creating a Separate Partition for Data Storage and MySQL Storage

Perform the following tasks to create a separate partition for data (block) storage and MySQL Storage

The following partitioning options are available:

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

Perform the following tasks to create the partition for data storage MySQL Storage.

1. Run the following command to create a directory to mount the partition:

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

2. Adjust /etc/fstab to mount the data storage partition. For example:

```
For example,this entry may vary based on the environment:
LABEL=PLD_DATA /opt/oracle/ocsm/var/vsi xfs
defaults,nosuid,nodev,nofail 0 2
LABEL=MYSQL_DATA /var/lib/mysql xfs
defaults,nosuid,nodev,nofail 0 2
```

During the MySQL and OCSM installation, partitions are detected by the product and the system uses these separate partitions.

Tasks to be Performed after RPM Installation

Perform the tasks given here after the

1. 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

2. Adjust the firewalld to access the Session Monitor applications by doing the following tasks:

   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 these tasks:

   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
   ```

   > **Note:**
   >
   > Please note that the ports 4740/4742 are the preferred ports for connecting to SBC / standalone probes respectively. So, the firewall should be opened for ports 4739/4741 only if you are agree to have non-TLS connections.

3. Reload the configuration by running the following command: `firewall-cmd --reload`

   > **Note:**
   >
   > If you are planning to enable additional services, see the discussion about network security in Oracle Communications Session Monitor Security Guide for a complete list of services and their respective ports.

4. Enable or Disable SELinux as per your requirement. For more information, see Enabling SELinux.

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:

1. 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
```

2. Reboot the system using the command:

```
reboot
```

3. 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
```

4. 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
```

Troubleshooting Tips

Following intructions will be helpful in solving issues in configuring SELinux.

To modify the mode in which SELinux runs in real-time, run the following commands:

Table 2-1   Modifying SELinux Mode

Mode	Command
To run SELinux in **permissive** mode (System prints warnings only but does not enforce SELinux policy)	`setenforce 0`
To run SELinux in the **enforcing** mode (SELinux security policy is enforced)	`setenforce 1`

Table 2-1   (Cont.) Modifying SELinux Mode

Mode	Command
Verify the status using command	`getenforce`

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>
```

Configuring Reverse Proxy Server

> **Note:**
>
> Configuring reverse proxy server is optional.

The Session Monitor services are available to you through a reverse proxy web server. By default, the Session Monitor comes with a bundled copy of NGINX, the configuration files located at /opt/oracle/ocsm/etc/nginx file. However, you may choose to use another web server, such as Apache. A sample configuration file for Apache 2.4 is located at /opt/oracle/ocsm/etc/httpd/conf.d/pld.conf file.

Run the following commands to install the Apache Web Server and mod_ssl packages:

```
yum install -y httpd mod_ssl
```

After installing Apache, run the following commands to enable Apache as a front-end web server instead of NGINX:

```
systemctl stop pld-nginx.service
systemctl disable pld-nginx.service
ln -sf /usr/lib/systemd/system/{httpd,pld-webserver}.service
```

```
cp /opt/oracle/ocsm/etc/httpd/conf.d/pld.conf /etc/httpd/conf.d/
mv /etc/httpd/conf.d/ssl.conf{,.orig}
systemctl daemon-reload
systemctl start httpd.service
systemctl enable httpd.service
```

If you choose to authenticate users at the level of the reverse proxy, you must uncomment the sections in the sample Apache configuration file which configures LDAP or RADIS authentication for the `/me/` and `/mec/` routes, and modify them as appropriate for your authentication provider. Additionally, you must enable external authentication in the Mediation Engine and the Mediation Engine Controller. See the discussion on external authentication in the *Operations Monitor User's Guide*.

Configuring Apache for Authenticating with LDAP Service

The NGINX Web Server provided with Session Monitor does not support the external authentication.
To enable external authorization you are required to have NGINX Web Server that provides external authentication and is optional. You can also have a webserver that supports External Authentication like Apache.

The default installation supports IPv6 only. Configurations are necessary for proxies and repos. If there are any, see Configuring Proxies and Repos.

> **Note:**
>
> On a SELinux enabled machine, for External Authentication, do not copy any modified `pld.conf` file from a different location and replace it with an existing file as SELinux blocks access to such files.
>
> Instead, edit the `pld.conf` file contents directly using the VI editor.

The following procedure explains configuring external authentication using Apache Web Server as it is widely used.

To configure Apache in Session Monitor for authenticating with LDAP service:

1. Login to Session Monitor.

2. Click **Admin** and select **Settings**.

3. Enable the setting, **External authentication** enabled and set it to **True**.

4. Logout from Session Monitor.

5. If the current web service is NGINX, change to HTTPD by following all the steps mentioned in Configuring Reverse Proxy Server.

   • Run the following commands to install the Apache Web Server and mod_ssl packages:

   ```
   yum install -y httpd mod_ssl
   ```

> **Note:**
>
> If you have proxy server, to complete download, edit the proxy settings for the external downloads to be successful.

> **Note:**
>
> Install Apache Web Server and **mod_ssl** packages together as the httpd package executes a post-install script which uses **mod_ssl** for generating a localhost certificate. The certificate is required for the default httpd service configuration. If the certificate is not generated, enter the following lines in the `/etc/httpd/conf.d/ssl.conf` file to start the httpd server:
>
> ```
> SSLCertificateFile /etc/pki/tls/certs/localhost.crt
> SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
> ```

If the localhost certificates are not generated, perform the following workaround to start the Apache server:

* Remove the **ssl.conf** file from the **/etc/httpd/conf.d** file.

6. Run the following commands to install all additional packages:

```
yum groupinstall "Development Tools" -y
```

7. Run the following command to install the required ldap modules:

```
yum install mod_ldap
```

8. Edit the pld.conf file:

```
vi /etc/httpd/conf.d/pld.conf
```

9. Edit the following location in the file as below:

```
  <LocationMatch "^/me/(?!(proxy/|c/|r/|scripts/|/help/|
logout\.html)).*$">
        #
        # BEGIN LDAP Auth
        # Uncomment and adjust the lines below for LDAP Auth
         RewriteEngine On
         RewriteCond %{SERVER_PORT} 443
         RewriteCond %{LA-U:REMOTE_USER} (.+)
         RewriteRule .* - [E=RU:%1,L]
         AuthType basic
        # AuthName should be the same as for /me/logout.html
         AuthName "OCSM COM"
         AuthBasicProvider ldap
         AuthLDAPURL "ldap://ldap-server/dc=example,dc=org?uid?one"
         AuthLDAPBindDN "cn=admin,dc=example,dc=org"
```

```
       AuthLDAPBindPassword <password>
       RequestHeader unset X-Forwarded-User
       RequestHeader set X-Forwarded-User %{RU}e
      # RequestHeader set X-Forwarded-User-Role ""
      # RequestHeader set X-Forwarded-User-Role
{AUTHENTICATE_employeeType}e
      # RequestHeader unset X-Forwarded-User-Permission
      # RequestHeader set X-Forwarded-User-Permission %
{AUTHENTICATE_gecos}e
      # # Admin permission mask - all bits set
      # RequestHeader set X-Forwarded-User-Permission
4610266613338864839
       Require valid-user
      # END LDAP AUTH
</Location>
```

For a description of the parameters and information on the optional parameters in the pld.conf file, see pls.conf File Details.

> **Note:**
>
> All Non admin users are required to be created on OCOM first and then these users can login via LDAP Authentication. However if permissions and roles are needed to be added for a user in LDAP, then these should be taken from OCOM MySQL Database for the User and use them to provision on LDAP. This is optional.

10. If you have modified the `Auth Name` above, then modify the `Auth Name` in this section in the `pld.conf`

```
 # Logout page for COM
   <Location /me/logout.html>
       AuthType basic
       # AuthName should be the same as for /me/
       AuthName "OCSM COM"
       AuthBasicProvider file
       AuthUserFile     "/opt/oracle/ocsm/etc/httpd/logout.htpasswd"
       Require          valid-user
       ProxyPass !
   </Location>
```

11. Run the following command to start and enable the httpd

```
systemctl restart httpd.service
```

The httpd server of Session Monitor has been configured for external authentication.

When you open the Session Monitor in web browser, the external authentication pop-up appears. On providing the correct LDAP user credentials, the user will be logged in successfully.

pld.conf File Details

Configuring Apache for Authenticating with LDAP Service requires you to edit the `pld.conf` file. Here, you can find the descriptions for the parameters that are edited and the optional parameters.

Table 2-2   pld.conf file parameters

Parameters	Description
<LDAP_Server>	The LDAP server name
"ldap://ldap-server/dc=example,dc=org?uid?one"	The LDAP server IP address to which the authentication request is sent by Session Monitor. As DC and CN are LDAP specific, check the DC and CN values with your Local LDAP configuration.
<password>	The password for LDAP server to which authentication to the specific user is to be processed. It should be a Hashed Password.
AuthName	"OCSM COM" is the default name provided. It can be modified to any convenient name.
{AUTHENTICATE_gecos}e (optional)	`gecos` is a parameter on your LDAP Server that stores the permissions for the user. As this is LDAP specific, check your local LDAP configuration. If permissions are defined for your user, then you can umcomment this line and change the parameter name from gecos to the appropriate name defined in your LDAP. When you log in, OCOM validates the permission received and then allows User Login.
{AUTHENTICATE_employeeType}e	Parameter on your LDAP Server that stores the Role for the User. As this is LDAP specific, check with your local LDAP configuration. If roles are defined for your user, then you can umcomment this line and change the parameter name from employee to the appropriate name defined in your LDAP. When you log in, OCOM validates the role received and then allows User Login.

Configuring Secure LDAP (LADPS) Support

To configure LDAPS support, follow these steps:

Follow the instructions given in Configuring Apache for Authenticating with LDAP Service before executing the following steps to configure LDAPS:

1. Copy the CA certificate from the LDAP server and place it in a directory other than / root.

   ```
   /opt/certs/<CA Certificate>
   ```

2. Assign permissions for the directory which has the CA certificate.

```
chmod -R 777 /opt/certs
```

3. Modify the `/etc/hosts` file with a fully qualified DNS.

```
<DNS-IP> <Host Name> <Fully Qualified Host Name>
```

4. Modify `/etc/httpd/conf.d/pld.conf` to have the following line after **CustomLog**:

```
LDAPTrustedGlobalCert CA_BASE64 </opt/certs/<CA Certificate>
```

5. Modify the **AuthLDAPURL** URL from ldap to ldaps.

```
AuthLDAPURL ""ldaps ://ldap-server/dc=example,dc=org?uid?one""
```

Configuring External Authentication for Session Monitor with Radius Service

This section explains how to configure the external authentication for Session Monitor with Radius Service using Apache Web Server.

For more information, refer to the following sections for configuring External Authentication with RADIUS service.

Troubleshooting External Authentication Issues for RADIUS on an SELinux Machine

On an SELinux-enabled machine, do not copy any modified `pld.conf` file from a different location and replace it with the existing file, as SELinux blocks access to such files. Instead, edit the `pld.conf` file contents directly using the vi/vim editor.

On an SELinux enabled machine, for External Authentication with the RADIUS Server, after copying the `mod_auth_xradius.so` file to the directory `/usr/lib64/httpd/modules/`, execute the this command to prevent SELinux from blocking access:

```
chcon -t httpd_modules_t /usr/lib64/httpd/modules/mod_auth_xradius.so
```

On a SELinux enabled machine, for External Authentication with Radius, perform the following tasks if you encounter this error after restarting HTTPD: `Permission denied: xradius: Cannot create DBM Cache at `/var/authxcache'`.

```
chcon -R -t httpd_cache_t /var/authxcache.dir
chcon -R -t httpd_cache_t /var/authxcache.pag
systemctl restart httpd.service
```

Configuring Apache for Authenticating with RADIUS Server

This section explains how to configure the external authentication for Session Monitor with the Radius Service using the Apache Web Server.

1. Login to Session Monitor

2. Click **Admin** and select **Settings**.

3. Enable the setting, **External authentication enabled** and set it to **True**.

4. **Logout** from Session Monitor.

5. If the current web service is NGINX, change to HTTPD by following the steps mentioned in Configuring Reverse Proxy Server.

    a. Run the following commands to install the Apache Web Server and mod_ssl packages:

    ```
    yum install httpd mod_ssl
    ```

    > **Note:**
    >
    > If you have a proxy server, to complete the download, edit the proxy settings for the external downloads to be successful.

    b. Install the Apache Web Server and `mod_ssl packages` together as the HTTPD package executes a post-install script that uses `mod_ssl` to generate a localhost certificate. The localhost certificate is required for the default HTTPD service configuration. If the certificate is not generated, enter the following lines in the `/etc/httpd/conf.d/ssl.conf` file to start the HTTPD server:

    ```
    SSLCertificateFile /etc/pki/tls/certs/localhost.crt
    SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
    ```

6. If the localhost certificates are not generated, remove the `ssl.conf` file from the `/etc/httpd/conf.d` file to start the Apache server.

7. Run the following commands to install all additional packages:

    ```
    yum groupinstall "Development Tools"
    yum install httpd-devel
    ```

8. To install Apache modules for Radius authentication, run the following commands:

    ```
    wget http://www.outoforder.cc/downloads/mod_auth_xradius/
    mod_auth_xradius-0.4.6.tar.bz2
    tar -xvf mod_auth_xradius-0.4.6.tar.bz2
    cd mod_auth_xradius-0.4.6
    ```

9. A code change is required in the `xradius_cache.c` file, for the module to install properly:

    ```
    $ vi /root/mod_auth_xradius-0.4.6/src/xradius_cache.c
    ```

10. Copy the following lines into the editor and press the ENTER key:

```
:%s/unixd_config/ap_unixd_config/g
```

11. Save the file.

12. To install the module files successfully, run the following commands:

```
$ ./configure --with-apxs=/sbin/apxs
$ make
$ make install
$ cd ..
```

13. Ensure that the `mod_auth_xradius.so` file is present in the `/usr/lib64/httpd/modules/` directory of your machine.

```
#ls -lrt /usr/lib64/httpd/modules/mod_auth_xradius.so
-rwxr-xr-x. 1 root root 193976 Mar 20 13:27 /usr/lib64/httpd/modules/
mod_auth_xradius.so
```

14. To load the required modules into the HTTPD configuration, edit the file `/etc/httpd/conf/httpd.conf` and paste the following lines. Better to put under any 'Load Module' section or under any commented 'Load module' sample code) and save the file.

```
LoadModule auth_xradius_module /usr/lib64/httpd/modules/
mod_auth_xradius.so
AuthXRadiusCache dbm /var/authxcache
```

15. Edit the `pld.conf` file:

```
vi /etc/httpd/conf.d/pld.conf
```

16. Edit the following location in the file as below:

```
<LocationMatch "^/me/(?!(proxy/|c/|r/|scripts/|/help/|logout\.html)).*$">
        #
        # BEGIN LDAP Auth
        # Uncomment and adjust the lines below for LDAP Auth
         AuthName "OCSM COM"
         AuthType basic
       AuthXRadiusAddServer "<Radius Server IP>:1812" "<Radius Shared
Secret>"
        AuthXRadiusTimeout 2
        AuthXRadiusRetries 2
        AuthBasicProvider xradius
        Require valid-user
        RewriteEngine On
        RewriteCond %{SERVER_PORT} 443
        RewriteCond %{LA-U:REMOTE_USER} (.+)
        RewriteRule .* - [E=RU:%1,L]
       # AuthName should be the same as for /me/logout.html
       # AuthLDAPURL "ldap://ldap-server/dc=example,dc=org?uid?one"
       # AuthLDAPBindDN "cn=admin,dc=example,dc=org"
       # AuthLDAPBindPassword admin
```

```
     RequestHeader unset X-Forwarded-User
     RequestHeader set X-Forwarded-User %{RU}e
    # RequestHeader set X-Forwarded-User-Role ""
    # RequestHeader set X-Forwarded-User-Role %
{AUTHENTICATE_employeeType}e
    # RequestHeader unset X-Forwarded-User-Permission
    # RequestHeader set X-Forwarded-User-Permission %
{AUTHENTICATE_gecos}e
    # # Admin permission mask - all bits set
    # RequestHeader set X-Forwarded-User-Permission
4610266613338864839
    # Require valid-user
  # END LDAP Auth
</LocationMatch>
```

> **Note:**
>
> For MEC make similar changes under section <LocationMatch "^/mec/
> ((?!(proxy/|r/|res/|help/|logout\.html)).*)$">

.

17. For a description of the parameters and information on the optional parameters in the RADIUS pld.conf file, see RADIUS pld.conf File Details.

> **Note:**
>
> All Non admin users are required to be created on OCOM first and then these users can login via RADIUS Authentication.

18. If you have modified the Auth Name above, then modify the Auth Name in this section in the `pld.conf` file.

```
# Logout page for COM
    <Location /me/logout.html>
        AuthType basic
        # AuthName should be the same as for /me/
        AuthName "OCSM COM"
        AuthBasicProvider file
        AuthUserFile     "/opt/oracle/ocsm/etc/httpd/
logout.htpasswd"
        Require         valid-user
        ProxyPass !
    </Location>
```

> **Note:**
>
> Change the AuthName directive for ME in <Location /me/logout.html> and for MEC in <Location /mec/logout.html>

19. Run the following command to start and enable the HTTPD:

```
systemctl daemon-reload
systemctl restart httpd.service
```

The HTTPD server of Session Monitor has been configured for external authentication with RADIUS. When you open the Session Monitor in web browser, the external authentication pop-up appears. On providing the correct RADIUS user credentials, the user will be logged in successfully.

RADIUS pld.conf File Details

Edit the `pld.conf` file. Here, you can find the descriptions for the parameters that are edited and the optional parameters.

Table 2-3   RADIUS pld.conf file parameters

Parameters	Descrption
AuthXRadiusTimeout	The number of seconds to wait response from RADIUS Server.
AuthXRadiusRetries	The number of attempts to connect to server, expressed as positive integer value. Number of retries multiplied by timeout value should not exceed 30 (seconds)
AuthName	"OCSM COM" is the default name provided. It can be modified to any convenient name.
AuthBasicProvider	Type of authentication to use
<Radius Shared Secret>	This field must contain the secret that will be shared by Operations Monitor and the RADIUS server used for authentication.
<Radius Server IP>	The address of the RADIUS server against which Operations Monitor performs authentication.

Session Monitor Post-Installation Tasks

This section provides instructions for the post-installation tasks for Session Monitor.

Before starting the post-installation tasks, verify that Session Monitor installation tasks are completed and all components are installed. See Installing Session Monitor Using the RPM.

About the Platform Setup Application

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:

1. Accept the license agreement to proceed with the Platform Setup Application.

2. The menu on the right shows your progress during configuration.

3. 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.

4. 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* **/setup/**, 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.

5. 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.

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:

1. In a web browser, go to https://<ip_address>/setup.

   The **Platform Setup Application Login** page appears.

2. In the **Username** field, enter **sysadmin** and in the **Password** field, enter **oracle**.

   The License Terms agreement page appears.

3. Accept each Session Monitor application license terms agreement, by selecting the **I agree to the license terms** check box.

4. Click **Proceed**.

   The **Change Password** dialog box appears.

   The **Platform Setup Application** page appears.

5. Change the password by doing the following:

   a. In the **Set password** field, enter a new password.

   > **Note:**
   >
   > The password must have at least 8 characters. The password must contain at least one uppercase character. The password must contain a number. The password must contain a special character (@, #, -, _, .).

   b. In the **Repeat password** field, re-enter the password used in the previous step, which verifies that the password value was entered correctly.

   c. Click **Change**.

   The **Machine Type** page appears.

6. On the Machine Type page, select the machine type on which to install your licensed Session Monitor applications and components:

- To install an Operations Monitor probe, select **Standalone Probe**.

- 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.

> **Note:**
>
> The Machine Type page only appears the first time you configure Session Monitor prior to the products installation. Machine type cannot be changed after the PSA installation is completed.
>
> You can select only one machine type for each installation process.
>
> Packet Inspector probe is not supported on a Session Monitor probe with SIP/RTP sniffing for the calls and VQ analysis.
>
> The products are machine-type specific and cannot be interchanged between machine types.
>
> For example, the Probe machine type requires a probe product, and the Mediation Engine machine type requires the Operations Monitor product.
>
> The machine type Mediation Engine Probe (embedded) must be chosen either with Operation Monitor or with Control Plane Monitor option selected.

7. 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.

8. 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.

> **Note:**
>
> The number entered in the Concurrent RTP streams field can cause performance and stability issues if it is set higher than what your network hardware supports. Values above 20 are not recommended. Changes to the RTP recording setting take effect only after restarting the system.

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.

> **Note:**
>
> You cannot change the configured extensions after the installation. All Oracle Communications Session Monitor Enterprise users should select Media quality .

9. Click Continue.

The Disk Usage page appears.

10. On the Disk Usage page, specify the maximum disk usage partition for the Packet Inspector.

> **Note:**
>
> On the Disk Usage page, specify the maximum disk usage partition for the shared file system containing the database/data storage (single raid systems). For systems with two raid arrays you can select the usage independently for both filesystems. For Probes with Packet Inspector feature you would be able to select the maximum storage capacity.

The ME Connection List page appears.

> **Note:**
>
> The **ME Connection List** page appears only if you have selected machine type as Probe or Mediation Engine with Probe.

11. (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 check box 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 un-encrypted Cleartext. A mediation engine can connect to more than one Operations Monitor Probe or more than one Session Border Controller Probe.

> **Note:**
>
> Oracle recommends using TLS for connections between Standalone Probes and the Mediation Engine.

12. Click **Continue**.

The Trusted Certificate page appears.

13. 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.

14. 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:

- To use the self-signed certificate, click **Continue**.

- To sign the server certificate with your organization's Public Key Infrastructure (PKI):

    a. Select **Download request**.

    b. Sign the certificate with the X.509 format.

    c. In the **Upload signed certificate** field, select **Browse** and locate the signed certificate file.

    d. Click **Continue**. The SMTP Configuration page appears.

> **Note:**
>
> – To regenerate a key and certificate on install, select **Regenerate key and self-signed certificate on install** and click **Continue**.
>
> – (Optional) Click **Download current certificate** to download the current self-signed certificate.

15. 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.

16. Click **Continue**.

    The Capture Settings page appears.

17. 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 8.

18. 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.

19. Click **Continue**.

    The Install page appears.

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

21. Open the **psa_conf.json** configuration file and verify your settings.

22. Click **Install**.

    The **Did you select the right applications** dialog box appears.

23. 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.

24. 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**.

25. 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.

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

4. Connect the cloned probe to the Mediation Engine and make sure that the connection is successful.

   > **Note:**
   >
   > Connect the cloned probe to the Mediation Engine only after changing the UUID. The cloned probe newly connected to the ME must be of the same version as the ME. For example, if the ME is on Release 5.1 version, then the probe version must also be Release 5.1 version.

3
Installing Session Monitor Offline

This chapter describes how to install Oracle Communications Session Monitor without an internet connection.

Downloading the RPMs

This section describes how to download the RPMs needed to install Session Monitor.

You can manually download all RPMs from https://yum.oracle.com/oracle-linux-8.html or use a script. See Dependency RPMs for information on which RPMs to download.

1. Download the `Download_rpms.sh` script from the software.zip file and save to your system. This script downloads all dependency RPMs except for OCSM and MySQL RPMs. See the Session Monitor Release Notes for information on downloading OCSM and MySQL RPMs:

2. Set execute permission as:

   ```
   chmod +x Download_rpms.sh
   ```

3. Run the following command to download the script:

   ```
   ./Download_rpms.sh
   ```

4. If you need to configure a proxy server for your system, run the same command with the following information:

   ```
   ./Download_rpms.sh "[PROTOCOL://]HOST[:PORT]"
   ```

Configuring the Repository Server

This section describes how to configure the repo server in order to install Session Monitor.

1. Copy the RPMs to the repo server in a temporary directory, such as `/tmp/ocsm/`.

2. Install the following RPMs in this order:

   a. rpm -ivh vsftpd-3.0.3-35.el8.x86_64.rpm

   b. rpm -ivh drpm-0.4.1-3.el8.x86_64.rpm

   c. rpm -ivh createrepo_c-libs-0.17.7-6.el8.x86_64.rpm

   d. rpm -ivh createrepo_c-0.17.7-6.el8.x86_64.rpm

3. Move the `/tmp/ocsm/` directory to `/var/ftp/pub/` by running the following command:

   ```
   mv /tmp/ocsm/  /var/ftp/pub/
   ```

4. Copy rpms of OCSM and MySQL to /var/ftp/pub/ocsm/.

> **Note:**
>
> The OCSM dependencies used here are based on MySQL 8.0.32. If
> there are any additional dependencies required, take that as well.

```
mysql-commercial-backup-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-client-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-client-plugins-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-common-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-devel-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-icu-data-files-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-libs-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-server-8.0.32-1.1.el8.x86_64.rpm
mysql-commercial-test-8.0.32-1.1.el8.x86_64.rpm
```

OCSM, MySQL, and other dependency RPMs are now located
in `/var/ftp/pub/ocsm/`.

5. Create the repo by running the following command:

```
createrepo  /var/ftp/pub/ocsm/
```

6. Add a comment in front of the root line of `/etc/vsftpd/ftpusers` and `/etc/vsftpd/user_list` using "#" to say the following:

```
[root@test vsftpd]# cat /etc/vsftpd/ftpusers
# Users that are not allowed to login via ftp
#root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody


[root@test vsftpd]# cat /etc/vsftpd/user_list
# vsftpd userlist
# If userlist_deny=NO, only allow users in this file
# If userlist_deny=YES (default), never allow users in this file,
and
# do not even prompt for a password.
# Note that the default vsftpd pam config also checks /etc/vsftpd/
ftpusers
# for users that are denied.
```

```
#root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news
uucp
operator
games
nobody
```

7. Disable SELinux by running the following commands:

```
setenforce 0
sed -i -e "s/^SELINUX=.*/SELINUX=disabled/" /etc/selinux/config
reboot
```

8. Using an editor, open the file `/etc/vsftpd/vsftpd.conf`.

9. Comment the line `anonymous_enable=NO`.

10. Save and quit the `vsftpd.conf` file.

11. Start the vsftp service by running the following commands:

```
systemctl start vsftpd
systemctl enable vsftpd
```

12. Check the status of vsftp service by running the following command:

```
systemctl status vsftpd
```

The status of the service should be active (running).

The repo server is ready to use.

Installing Oracle Communications Session Monitor for the First Time using the Above Configured Repo Server

This section describes how to install Session Monitor for the first time.

1. Login to the OCSM server as root or root privileged user.

2. Rename all repose under `/etc/yum.repos.d`

```
mv /etc/yum.repos.d/oracle-linux-ol8.repo /etc/yum.repos.d/oracle-linux-
ol8.repo_bkp
mv /etc/yum.repos.d/uek-ol8.repo /etc/yum.repos.d/uek-ol8.repo_bkp
mv /etc/yum.repos.d/virt-ol8.repo /etc/yum.repos.d/virt-ol8.repo_bkp
```

3. Create `/etc/yum.repos.d/ocsm.repo` with the following content:

```
[OCSM]
name=OCSM dependencies
baseurl=ftp://<REPO_SERVER_IP>/pub/ocsm/
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-oracle
gpgcheck=0
enabled=1
proxy=_none_
```

4. Clean up the repo by running the following command:

```
yum clean all
```

5. Verify the repolist by running the following command:

```
# yum repolist
repo id repo name
OCSM OCSM dependencies
```

6. Install the MySQL RPMs using the following command:

```
yum install mysql-commercial-*
```

7. Copy the following RPMs from the repo Server to the OCSM Server in a temporary directory, such as `/tmp/dependency/`and install the RPMs on OCSM Server in this order:

```
1. rpm -ivh python39-setuptools-
wheel-50.3.2-4.module+el8.5.0+20364+c7fe1181.noarch.rpm
2. rpm -ivh python39-pip-
wheel-20.2.4-7.module+el8.6.0+20625+ee813db2.noarch.rpm
3. rpm -ivh python39-
libs-3.9.13-2.module+el8.7.0+20879+a85b87b0.x86_64.rpm
4. rpm -ivh
python39-3.9.13-2.module+el8.7.0+20879+a85b87b0.x86_64.rpm
5. rpm -ivh python39-
pip-20.2.4-7.module+el8.6.0+20625+ee813db2.noarch.rpm
6. rpm -ivh python39-
pyyaml-5.4.1-1.module+el8.5.0+20364+c7fe1181.x86_64.rpm
```

8. Download the following protobuf package from https://pypi.org/project/protobuf/3.20.3/#files to a temporary directory, such as /tmp/dependency/ directory of OCSM Server:

```
protobuf-3.20.3-cp39-cp39-manylinux_2_5_x86_64.manylinux1_x86_64.whl
```

9. Download the following MySQL Connector package from MOS to same temporary directory used in Step 8, such as `/tmp/dependency/` directory of the OCSM Server.

```
MySQL Connector 8.0.32 Package: p34984522_800_Linux-x86-64.zip
(Patch 34984522: MySQL Connector/Python 8.0.32 WHL for portable Linux x86
(64bit) Python 3.9)
```

> **✎ Note:**
>
> The OCSM dependencies used here are based on MySQL Connector 8.0.32, as we are using MySQL 8.0.32 version. If there are any additional dependencies required, please take that as well.

10. Set python alternatives to python3.9 by running the following commands:

```
update-alternatives --config python3
update-alternatives --config python
```

> **✎ Note:**
>
> When prompted, select the number corresponding to python3.9 option and press the Enter key.

> **✎ Note:**
>
> After the OCSM Installation, while installing any new packages using yum, some packages will install Python 3.6 as a dependency. As a result Python alternatives will get changed. This can cause unexpected problems in the OCSM functionality. So it is mandatory for you to verify that Python is pointing to python 39 after every package installation using yum by running the above two commands.

11. From the temporary directory, such as `/tmp/dependency/`, run the following commands to install MySQL Connector:

```
cd /tmp/dependency/
yum install unzip
unzip p34984522_800_Linux-x86-64.zip
pip3 install mysql_connector_python-8.0.32-1commercial-cp39-cp39-
manylinux1_x86_64.whl --no-index --find-links=/tmp/dependency/
```

12. Install OCSM by running the following command:

```
yum -y install ocsm
```

OCSM Installation is now complete.

Installing Any New Package on the OCSM Server

Complete the tasks given in this section to install any new package on the OCSM server.

To install any new package on the OCSM Server:

1. Download the required RPM and their dependences from yum.oracle.com OL8 repo manually

2. Copy the RPMs to `/var/ftp/pub/ocsm/` location of the Repo Server.

3. On the Repo Server, execute the following command:

    ```
    createrepo /var/ftp/pub/ocsm/
    ```

4. On the OCSM Server, execute the following command:

    ```
    yum clean all
    ```

5. Install the package on the OCSM Server using the command:

    ```
    yum install <package>
    ```

    OR You can update the `Download_rpm.sh` script by putting the RPM names under the respective Repo links and follow the steps.

Dependency RPMs

This section describes the RPMs needed to install Session Monitor without an internet connection.

BaseOS Latest: https://yum.oracle.com/repo/OracleLinux/OL8/baseos/latest/x86_64/index.html.

1. bash-4.4.20-4.el8_6.x86_64.rpm

2. brotli-1.0.6-3.el8.x86_64.rpm

3. bzip2-libs-1.0.6-26.el8.x86_64.rpm

4. c-ares-1.13.0-6.el8.x86_64.rpm

5. coreutils-8.30-13.0.1.el8.x86_64.rpm

6. coreutils-single-8.30-13.0.1.el8.x86_64.rpm

7. dejavu-sans-fonts-2.35-7.el8.noarch.rpm

8. dejavu-serif-fonts-2.35-7.el8.noarch.rpm

9. freetype-2.9.1-9.el8.x86_64.rpm

10. glib2-2.56.4-159.0.1.el8.x86_64.rpm

11. glibc-2.28-211.0.1.el8.x86_64.rpm

12. gnutls-3.6.16-5.el8_6.x86_64.rpm

13. krb5-libs-1.18.2-22.0.1.el8_7.x86_64.rpm

14. libcap-2.48-4.el8.x86_64.rpm

15. libcurl-7.61.1-25.el8_7.1.x86_64.rpm

16. libcurl-minimal-7.61.1-25.el8_7.1.x86_64.rpm

17. libgcc-8.5.0-16.0.2.el8_7.x86_64.rpm

18. libgcrypt-1.8.5-7.el8_6.x86_64.rpm

19. libgomp-8.5.0-16.0.2.el8_7.x86_64.rpm

20. libibverbs-41.0-1.el8.x86_64.rpm

21. libicu-60.3-2.el8_1.x86_64.rpm

22. libnghttp2-1.33.0-3.el8_2.1.x86_64.rpm

23. libnl3-3.7.0-1.el8.x86_64.rpm

24. libpcap-1.9.1-5.el8.x86_64.rpm

25. libpng-1.6.34-5.el8.x86_64.rpm

26. libssh-0.9.6-3.el8.x86_64.rpm

27. libstdc++-8.5.0-16.0.2.el8_7.x86_64.rpm

28. libuuid-2.32.1-39.el8_7.x86_64.rpm

29. libxcrypt-4.1.1-6.el8.x86_64.rpm

30. libxml2-2.9.7-15.el8_7.1.x86_64.rpm

31. libzstd-1.4.4-1.0.1.el8.x86_64.rpm

32. lshw-B.02.19.2-6.el8.x86_64.rpm

33. numactl-devel-2.0.12-13.el8.x86_64.rpm

34. numactl-libs-2.0.12-13.el8.x86_64.rpm

35. openssl-1.1.1k-7.el8_6.x86_64.rpm

36. openssl-libs-1.1.1k-7.el8_6.x86_64.rpm

37. openssl-perl-1.1.1k-7.el8_6.x86_64.rpm

38. pciutils-3.7.0-1.el8.x86_64.rpm

39. pcre2-10.32-3.el8_6.x86_64.rpm

40. python3-requests-2.20.0-2.1.el8_1.noarch.rpm

41. python3-setuptools-39.2.0-6.el8.noarch.rpm

42. selinux-policy-3.14.3-108.0.2.el8_7.1.noarch.rpm

43. selinux-policy-targeted-3.14.3-108.0.2.el8_7.1.noarch.rpm

44. snappy-1.1.8-3.el8.x86_64.rpm

45. sudo-1.8.29-8.el8_7.1.x86_64.rpm

46. systemd-libs-239-68.0.2.el8_7.2.x86_64.rpm

47. xmlrpc-c-1.51.0-8.el8.x86_64.rpm

48. xmlrpc-c-client-1.51.0-8.el8.x86_64.rpm

49. xz-libs-5.2.4-4.el8_6.x86_64.rpm

50. unzip-6.0-46.0.1.el8.x86_64.rpm

ORACLE

51. zlib-1.2.11-21.el8_7.x86_64.rpm

52. libcom_err-devel-1.45.6-5.el8.x86_64.rpm

53. keyutils-libs-devel-1.5.10-9.el8.x86_64.rpm

54. libpkgconf-1.4.2-1.el8.x86_64.rpm

55. libkadm5-1.18.2-21.0.1.el8.x86_64.rpm

56. krb5-devel-1.18.2-21.0.1.el8.x86_64.rpm

57. libsepol-devel-2.9-3.el8.x86_64.rpm

58. libselinux-devel-2.9-6.el8.x86_64.rpm

59. libverto-devel-0.3.2-2.el8.x86_64.rpm

60. pcre2-devel-10.32-3.el8_6.x86_64.rpm

61. pcre2-utf16-10.32-3.el8_6.x86_64.rpm

62. openssl-devel-1.1.1k-7.el8_6.x86_64.rpm

63. perl-Carp-1.42-396.el8.noarch.rpm

64. pcre2-utf32-10.32-3.el8_6.x86_64.rpm

65. perl-Data-Dumper-2.167-399.el8.x86_64.rpm

66. perl-Errno-1.28-421.el8.x86_64.rpm

67. perl-Exporter-5.72-396.el8.noarch.rpm

68. perl-File-Path-2.15-2.el8.noarch.rpm

69. perl-File-Temp-0.230.600-1.el8.noarch.rpm

70. perl-Encode-2.97-3.el8.x86_64.rpm

71. perl-Getopt-Long-2.50-4.el8.noarch.rpm

72. perl-HTTP-Tiny-0.074-1.el8.noarch.rpm

73. perl-IO-1.38-421.el8.x86_64.rpm

74. perl-MIME-Base64-3.15-396.el8.x86_64.rpm

75. perl-PathTools-3.74-1.el8.x86_64.rpm

76. perl-Pod-Escapes-1.07-395.el8.noarch.rpm

77. perl-Pod-Perldoc-3.28-396.el8.noarch.rpm

78. perl-Pod-Simple-3.35-395.el8.noarch.rpm

79. perl-Pod-Usage-1.69-395.el8.noarch.rpm

80. perl-Scalar-List-Utils-1.49-2.el8.x86_64.rpm

81. perl-Socket-2.027-3.el8.x86_64.rpm

82. perl-Storable-3.11-3.el8.x86_64.rpm

83. perl-Term-ANSIColor-4.06-396.el8.noarch.rpm

84. perl-Term-Cap-1.17-395.el8.noarch.rpm

85. perl-Text-ParseWords-3.30-395.el8.noarch.rpm

86. perl-Text-Tabs+Wrap-2013.0523-395.el8.noarch.rpm

87. perl-Time-Local-1.280-1.el8.noarch.rpm

88. perl-Unicode-Normalize-1.25-396.el8.x86_64.rpm

89. perl-constant-1.33-396.el8.noarch.rpm

90. perl-macros-5.26.3-421.el8.x86_64.rpm

91. perl-interpreter-5.26.3-421.el8.x86_64.rpm

92. perl-parent-0.237-1.el8.noarch.rpm

93. perl-libs-5.26.3-421.el8.x86_64.rpm

94. perl-threads-2.21-2.el8.x86_64.rpm

95. perl-podlators-4.11-1.el8.noarch.rpm

96. perl-threads-shared-1.58-2.el8.x86_64.rpm

97. pkgconf-1.4.2-1.el8.x86_64.rpm

98. pkgconf-m4-1.4.2-1.el8.noarch.rpm

99. pkgconf-pkg-config-1.4.2-1.el8.x86_64.rpm

100. zlib-devel-1.2.11-20.el8.x86_64.rpm

101. python3-chardet-3.0.4-7.el8.noarch.rpm

102. python3-urllib3-1.24.2-5.0.1.el8.noarch.rpm

103. python3-idna-2.5-5.el8.noarch.rpm

104. net-snmp-libs-5.8-25.0.2.el8_7.1.x86_64.rpm

105. python3-pysocks-1.6.8-3.el8.noarch.rpm

106. lm_sensors-libs-3.4.0-23.20180522git70f7e08.el8.x86_64.rpm

107. dejavu-fonts-common-2.35-7.el8.noarch.rpm

108. fontpackages-filesystem-1.44-22.el8.noarch.rpm

109. libmetalink-0.1.3-7.el8.x86_64.rpm

110. cronie-1.5.2-8.el8.x86_64.rpm

111. tar-1.30-6.el8_7.1.x86_64.rpm

112. net-tools-2.0-0.52.20160912git.el8.x86_64.rpm

113. avahi-libs-0.7-20.el8.x86_64.rpm

114. binutils-2.30-117.0.3.el8.x86_64.rpm

115. checkpolicy-2.9-1.el8.x86_64.rpm

116. efivar-libs-37-4.el8.x86_64.rpm

117. elfutils-devel-0.187-4.el8.x86_64.rpm

118. elfutils-libelf-devel-0.187-4.el8.x86_64.rpm

119. environment-modules-4.5.2-2.el8.x86_64.rpm

120. glibc-devel-2.28-211.0.1.el8.x86_64.rpm

121. glibc-headers-2.28-211.0.1.el8.x86_64.rpm

122. kernel-headers-4.18.0-425.13.1.el8_7.x86_64.rpm

123. libbabeltrace-1.5.4-4.el8.x86_64.rpm

124. libgfortran-8.5.0-16.0.2.el8_7.x86_64.rpm

125. libquadmath-8.5.0-16.0.2.el8_7.x86_64.rpm

126. libtool-ltdl-2.4.6-25.el8.x86_64.rpm

127. libxcrypt-devel-4.1.1-6.el8.x86_64.rpm

128. libzstd-devel-1.4.4-1.0.1.el8.x86_64.rpm

129. make-4.2.1-11.el8.x86_64.rpm

130. mokutil-0.6.0-1.0.1.el8.x86_64.rpm

131. policycoreutils-python-utils-2.9-20.0.1.el8.noarch.rpm

132. python3-audit-3.0.7-4.el8.x86_64.rpm

133. python3-libsemanage-2.9-9.el8.x86_64.rpm

134. python3-policycoreutils-2.9-20.0.1.el8.noarch.rpm

135. python3-setools-4.3.0-3.el8.x86_64.rpm

136. tcl-8.6.8-2.el8.x86_64.rpm

137. xz-devel-5.2.4-4.el8_6.x86_64.rpm

138. zip-3.0-23.el8.x86_64.rpm

139. elfutils-debuginfod-client-devel-0.187-4.el8.x86_64.rpm

140. kernel-devel-4.18.0-425.13.1.el8_7.x86_64.rpm

AppStream Latest: https://yum.oracle.com/repo/OracleLinux/OL8/appstream/x86_64/index.html

1. python39-3.9.13-2.module+el8.7.0+20879+a85b87b0.x86_64.rpm

2. python39-libs-3.9.13-2.module+el8.7.0+20879+a85b87b0.x86_64.rpm

3. python39-pyyaml-5.4.1-1.module+el8.5.0+20364+c7fe1181.x86_64.rpm

4. python39-pip-20.2.4-7.module+el8.6.0+20625+ee813db2.noarch.rpm

5. python39-pip-wheel-20.2.4-7.module+el8.6.0+20625+ee813db2.noarch.rpm
python39-setuptools-wheel-50.3.2-4.module+el8.5.0+20364+c7fe1181.noarch.rpm

6. python39-setuptools-wheel-50.3.2-4.module+el8.5.0+20364+c7fe1181.noarch.rpm

7. libX11-1.6.8-5.el8.x86_64.rpm libjpeg-turbo-1.5.3-12.el8.x86_64.rpm

8. libjpeg-turbo-1.5.3-12.el8.x86_64.rpm

9. libmaxminddb-1.2.0-10.el8.x86_64.rpm

10. libsmi-0.4.8-23.el8.x86_64.rpm libtiff-4.0.9-26.el8_7.x86_64.rpm

11. libtiff-4.0.9-26.el8_7.x86_64.rpm

12. net-snmp-5.8-25.0.2.el8_7.1.x86_64.rpm

13. python3-reportlab-3.4.0-8.el8.x86_64.rpm

14. sbc-1.3-9.el8.x86_64.rpm

15. whois-5.5.1-2.el8.x86_64.rpm

16. vsftpd-3.0.3-35.el8.x86_64.rpm

17. drpm-0.4.1-3.el8.x86_64.rpm

18. createrepo_c-libs-0.17.7-6.el8.x86_64.rpm

19. createrepo_c-0.17.7-6.el8.x86_64.rpm

20. perl-JSON-2.97.001-2.el8.noarch.rpm

21. perl-Memoize-1.03-421.el8.noarch.rpm

22. perl-Time-HiRes-1.9758-2.el8.x86_64.rpm

23. libxcb-1.13.1-1.el8.x86_64.rpm

24. libwebp-1.0.0-5.el8.x86_64.rpm

25. python3-pillow-5.1.1-18.el8_5.x86_64.rpm

26. mariadb-connector-c-3.1.11-2.el8_3.x86_64.rpm

27. net-snmp-agent-libs-5.8-25.0.2.el8_7.1.x86_64.rpm

28. libXau-1.0.9-3.el8.x86_64.rpm

29. jbigkit-libs-2.1-14.el8.x86_64.rpm

30. fribidi-1.0.4-9.el8.x86_64.rpm

31. harfbuzz-1.7.5-3.el8.x86_64.rpm

32. libX11-common-1.6.8-5.el8.noarch.rpm

33. graphite2-1.3.10-10.el8.x86_64.rpm

34. lcms2-2.9-2.el8.x86_64.rpm

35. openjpeg2-2.4.0-5.el8.x86_64.rpm

36. whois-nls-5.5.1-2.el8.noarch.rpm

37. wget-1.19.5-10.0.1.el8.x86_64.rpm

38. gcc-toolset-11-11.1-1.el8.x86_64.rpm

39. boost-atomic-1.66.0-13.el8.x86_64.rpm

40. boost-chrono-1.66.0-13.el8.x86_64.rpm

41. boost-date-time-1.66.0-13.el8.x86_64.rpm

42. boost-filesystem-1.66.0-13.el8.x86_64.rpm

43. boost-regex-1.66.0-13.el8.x86_64.rpm

44. boost-system-1.66.0-13.el8.x86_64.rpm

45. boost-thread-1.66.0-13.el8.x86_64.rpm

46. boost-timer-1.66.0-13.el8.x86_64.rpm

47. cpp-8.5.0-15.0.1.el8.x86_64.rpm

48. ctags-5.8-22.el8.x86_64.rpm

49. gc-7.6.4-3.el8.x86_64.rpm

50. gcc-8.5.0-15.0.1.el8.x86_64.rpm

51. gcc-toolset-11-annobin-docs-10.23-1.el8.noarch.rpm

52. gcc-toolset-11-binutils-2.36.1-2.0.1.el8.x86_64.rpm

53. gcc-toolset-11-dwz-0.14-2.el8.x86_64.rpm

54. gcc-toolset-11-dyninst-11.0.0-2.el8.x86_64.rpm

55. gcc-toolset-11-elfutils-0.185-5.el8.x86_64.rpm

56. gcc-toolset-11-elfutils-debuginfod-client-0.185-5.el8.x86_64.rpm

57. gcc-toolset-11-elfutils-libelf-0.185-5.el8.x86_64.rpm

58. gcc-toolset-11-elfutils-libs-0.185-5.el8.x86_64.rpm

59. gcc-toolset-11-gcc-11.2.1-9.1.0.3.el8.x86_64.rpm

60. gcc-toolset-11-gcc-c++-11.2.1-9.1.0.3.el8.x86_64.rpm

61. gcc-toolset-11-gcc-gfortran-11.2.1-9.1.0.3.el8.x86_64.rpm

62. gcc-toolset-11-gdb-10.2-5.0.1.el8.x86_64.rpm

63. gcc-toolset-11-libquadmath-devel-11.2.1-9.1.0.3.el8.x86_64.rpm

64. gcc-toolset-11-libstdc++-devel-11.2.1-9.1.0.3.el8.x86_64.rpm

65. gcc-toolset-11-ltrace-0.7.91-1.el8.x86_64.rpm

66. gcc-toolset-11-make-4.3-2.el8.x86_64.rpm

67. gcc-toolset-11-perftools-11.1-1.el8.x86_64.rpm

68. gcc-toolset-11-runtime-11.1-1.el8.x86_64.rpm

69. gcc-toolset-11-strace-5.13-7.el8.x86_64.rpm

70. gcc-toolset-11-systemtap-4.5-6.el8.x86_64.rpm

71. gcc-toolset-11-systemtap-client-4.5-6.el8.x86_64.rpm

72. gcc-toolset-11-systemtap-devel-4.5-6.el8.x86_64.rpm

73. gcc-toolset-11-systemtap-runtime-4.5-6.el8.x86_64.rpm

74. gcc-toolset-11-toolchain-11.1-1.el8.x86_64.rpm

75. gcc-toolset-11-valgrind-3.17.0-6.el8.x86_64.rpm

76. guile-2.0.14-7.0.1.el8.x86_64.rpm

77. isl-0.16.1-6.el8.x86_64.rpm

78. libatomic_ops-7.6.2-3.el8.x86_64.rpm

79. libipt-1.6.1-8.el8.x86_64.rpm

80. libmpc-1.1.0-9.1.el8.x86_64.rpm

81. nspr-4.34.0-3.el8_6.x86_64.rpm

82. nss-3.79.0-10.el8_6.x86_64.rpm

83. nss-softokn-3.79.0-10.el8_6.x86_64.rpm

84. nss-softokn-freebl-3.79.0-10.el8_6.x86_64.rpm

85. nss-sysinit-3.79.0-10.el8_6.x86_64.rpm

86. nss-util-3.79.0-10.el8_6.x86_64.rpm

87. scl-utils-2.0.2-15.0.1.el8.x86_64.rpm

88. source-highlight-3.1.8-17.el8.x86_64.rpm

89. tbb-2018.2-9.el8.x86_64.rpm

90. gcc-toolset-11-gcc-gdb-plugin-11.2.1-9.1.0.3.el8.x86_64.rpm

91. gcc-toolset-11-binutils-devel-2.36.1-2.0.1.el8.x86_64.rpm

92. gcc-toolset-11-elfutils-libelf-devel-0.185-5.el8.x86_64.rpm

Developer EPEL Packages: https://yum.oracle.com/repo/OracleLinux/OL8/developer/EPEL/x86_64/index.html

1. gperftools-libs-2.7-9.el8.x86_64.rpm

2. jemalloc-5.2.1-2.el8.x86_64.rpm

3. openpgm-5.2.122-21.el8.x86_64.rpm

4. spandsp-0.0.6-9.el8.x86_64.rpm

5. zeromq-4.3.4-2.el8.x86_64.rpm

6. libimagequant-2.12.5-1.el8.x86_64.rpm

7. libraqm-0.7.0-4.el8.x86_64.rpm

8. libunwind-1.3.1-3.el8.x86_64.rpm

UEK Release 7 Packages: https://yum.oracle.com/repo/OracleLinux/OL8/UEKR7/x86_64/index.html

• kernel-uek-devel-5.15.0-3.60.5.1.el8uek.x86_64.rpm

4
Configuring Session Monitor

This chapter describes how to configure Oracle Communications Session Monitor.

About the Platform Setup Application

The Platform Setup Application (PSA) guides you through the configuration steps to get the Session Monitor system running, including configuring the machine type, capture settings, DNS settings, and SMTP settings.

The menu on the right shows your progress in the overall configuration.

Platform Setup Application Initial Log In

This section provides how to log into Platform Setup Application initially.

1. Open the web browser and enter the URL provided by the System Administrator.

2. Confirm the security exception to proceed.

   The Log in page appears.

3. Enter the **Username** and **Password**. For default username and password, contact your Oracle representative.

4. Click **Sign in**.

5. **Review and Accept** the license of the software to continue.

   The Platform Application Setup page appears.

Changing Your Password

1. Click your username in the top right corner.

2. Select **Change Password** from the drop-down menu.

3. Enter the old and the new passwords.

   Passwords must have the following characteristics:

   • At least 8 characters

   • At least one uppercase character

   • At least one digit

   • At least one special character

4. Click **Change**.

Restarting or Powering Off Session Monitor

The restart and power off buttons are accessible through the power button on the top right-hand corner of the screen.

Figure 4-1   Drop-Down Menu on Clicking the Power Button
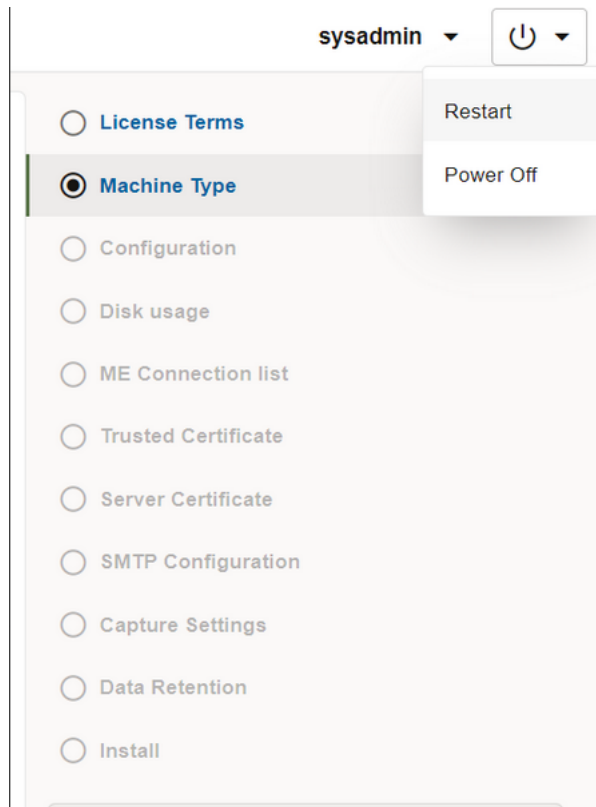
After selecting an option, you are prompted a final time to confirm that you wish to proceed.

Selecting the Machine Type

The following figure shows the Machine Type Settings page.

Figure 4-2   Machine Type Settings pages

The Machine Type Settings page allows you to select which products you want to install. This page only appears the first time you configure Session Monitor prior to the products installation.

Select your machine type by clicking **Probe** or **Mediation Engine** or **Aggregation Engine** button. This will enable the corresponding product selection.

Note:

- You can select only one machine type per installation.
- Packet Inspector is not supported on the machine collocated with Operations Monitor or Probe with SIP/RTP sniffing for the calls and VQ analysis.

Next, select the check boxes next to the products that you want to install. Only checked items are included in the installation.

> **Note:**
>
> The products are machine type specific and cannot be interchanged between machine types.
>
> For example, the Probe machine type requires a probe product, and the Mediation Engine machine type requires the Operations Monitor product.

After selecting the products, click **continue** to proceed with the installation. Your machine type and product selections should appear in the status panel located on the right under the navigation menu.

Configuring Session Monitor

This step in the configuration process allows you to configure Session Monitor settings for this machine in accordance with the terms of your license.

> **Note:**
>
> If you do not have a valid Session Monitor license, contact Oracle.

Figure 4-3   Configuration page

On the left side of the page you must enter the number of concurrent calls printed on your license. On the right side you must check the product extensions you have a license to use. All enterprise customers should automatically check **Media quality**.

> **Note:**
>
> The number of Concurrent RTP streams can cause performance and stability issues if it is set higher than the hardware and the network permits. Values above 20 are not recommended. Changes to the RTP recording setting take effect only after a restart of the system. If you have multiple servers involved in your set up (additional standalone Probes servers connected to the Mediation Engine), this setting must be set on each Probe (unless certain Probe is not sniffing Media so that RTP recording is not really applicable for the Probe). In such scenarios, the value that is set should be same on each node, on the Mediation Engine (or the Mediation Engine with local Probe), and the Probes.

Click the **continue** button to navigate to the ME Connection List page.

Mediation Engine Connection List

For a Probe machine type, the Mediation Engine Connection List page allows you to configure which Mediation Engines the Operations Monitor Probe connects to.

The following figure shows the ME Connection List page.

The Operations Monitor Probe can connect to one or more Mediation Engines, using TLS encryption, or with some configurations, also cleartext. Likewise, a Mediation Engine can connect to more than one Operations Monitor Probe (as well as Session Border Controller Probes).

On the Mediation Engine, cleartext connections are usually on port 4741 and encrypted connections on port 4742. For encrypted connections, the Operations Monitor Probe and the Mediation Engine need to be able to verify the certificate of the other party.

Figure 4-4   List of Mediation Engines

List of Mediation Engines

List of Mediation Engines that can connect to this Probe. Its possible to add new ones and existing ones can be edited or removed.

List of Mediation Engines

Add a new ME	Edit				Remove
TLS	**Port**	**Host**	**Name**	**Connection**	
No	4741	127.0.0.1	local	n/a	

Reset changes

Continue

The Mediation Engine machines by default only accept encrypted connections (unless the Mediation Engine and Probe are on the same machine); for unencrypted connections the check box Accept insecure connections from remote probes on the Trusted Certificate page must be checked.

The following figure shows the Trusted Certificate page.

Figure 4-5   Trusted Certificate page
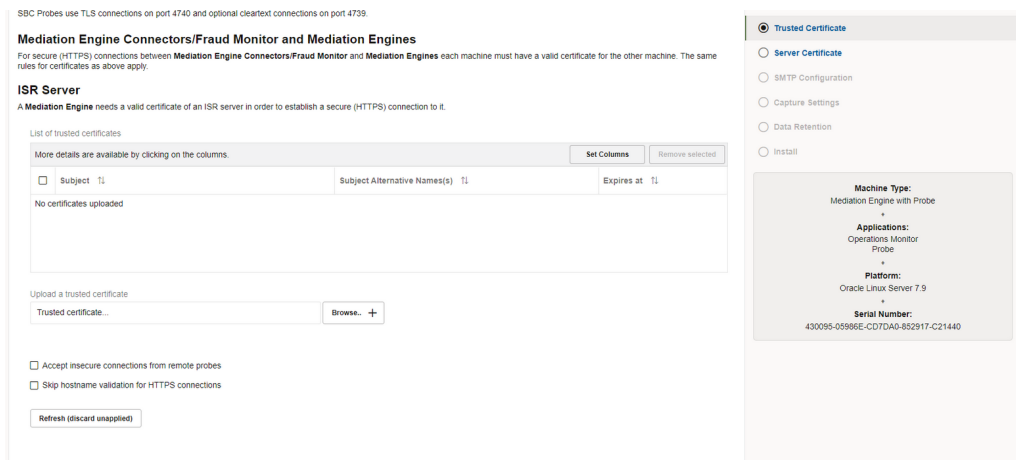
Typical Connection Scenarios

Mediation Engine and Operations Monitor Probe Are on the Same Machine

For setups with a Mediation Engine machine with an embedded Probe, a cleartext connection is automatically added to the ME connection list. For cleartext connections, no certificates are exchanged.

One Mediation Engine and Two Operations Monitor Probes

For setups with one Mediation Engine and two Operations Monitor Probes, the self-signed server certificates of both Operations Monitor Probes are uploaded as trusted certificates on the Mediation Engine, and the self-signed server certificate of the Mediation Engine is uploaded on both Operations Monitor Probes as a trusted certificate. On each Operations Monitor Probe, the IP of the Mediation Engine is added to the ME connection list with TLScheck box selected.

The following table describes the actions to configure the connections between one Mediation Engine and two Operations Monitor Probes.

Table 4-1   One Mediation Engine and Two Operations Monitor Probes

Machine	Action
Mediation Engine	• Download the Server Certificate. • Upload the Server Certificate of the Operations Monitor Probe1 to Trusted Certificate. • Upload the Server Certificate of the Operations Monitor Probe2 to Trusted Certificate.
Operations Monitor Probe 1	• Download the Server Certificate. • Upload the Server Certificate of the Mediation Engine to Trusted Certificate. • Add IP of the Mediation Engine to the ME Connection List, with TLS connection.
Operations Monitor Probe 2	• Download Server Certificate. • Upload Server Certificate of the Mediation Engine to Trusted Certificate. • Add IP of Mediation Engine to ME Connection List, with TLS connection.

Two Mediation Engines and One Operations Monitor Probe

For setups with two Mediation Engines and one Operations Monitor Probe, the self-signed server certificate of the Operations Monitor Probe is uploaded as trusted certificate on both Mediation Engines, and the self-signed server certificates of the Mediation Engine are uploaded on the Operations Monitor Probe as a trusted certificate. On the Operations Monitor Probe, the IPs of the Mediation Engines are both added to the ME connection list with TLScheck box selected.

The following table describes the actions to configure the connections between two Mediation Engines and one Operations Monitor Probe.

Table 4-2   Two Mediation Engines and One Operations Monitor Probe

Machine	Action
Mediation Engine 1	• Download the Server Certificate. • Upload the Server Certificate of the Operations Monitor Probe to Trusted Certificate.
Mediation Engine 2	• Download the Server Certificate. • Upload the Server Certificate of the Operations Monitor Probe to Trusted Certificate.
Operations Monitor Probe	• Download the Server Certificate. • Upload the Server Certificate of Mediation Engine 1 to Trusted Certificate. • Upload the Server Certificate of Mediation Engine 2 to Trusted Certificate. • Add IP of Mediation Engine 1 to ME Connection List, with TLS connection. • Add IP of Mediation Engine 2 to ME Connection List, with TLS connection.

All Other Scenarios

For setups with more than two Operations Monitor Probes or Mediation Engines, Oracle recommends that you use PKI (Public Key Infrastructure) with root certificates as described in *Oracle Communications Session Monitor Security Guide*.

Trusted Certificates

The Trusted Certificates page is used to configure the authentication of session border controllers (SBCs). This step is necessary before attempting to connect SBCs to Session Monitor.

For secure (HTTPS) connections between Mediation Engine Connectors and Mediation Engines each machine must have a valid certificate for the other machine. The same rules for certificates as for ME and Probe.

ISR Server

A Mediation Engine requires a valid certificate of an ISR server in order to establish a secure (HTTPS) connection to it.

Fraud Monitor

For secure (HTTPS) connections between Fraud Monitor and Mediation Engine, each machine must have a valid certificate for the other machine. The same rules for certificates as for ME and Probe.

For more information, see the discussion about connection with Oracle Session Border Controller in *Session Monitor Security Guide*.

Configuring the SMTP Settings

The following figure shows the SMTP Configuration page.

Figure 4-6   SMTP Configuration page

Session Monitor can send notifications and alerts directly to users' email addresses. Which notification to send to which address is configured in the relevant products. However, you first need to configure the SMTP settings properly for this feature to be available.

Setting Up the Mail Server

To use the email notification feature, select **Enable SMTP** check box. The system needs an SMTP server to send emails. Contact your network administrator to find out the address of the server your organization uses. The default port is the standard port 25.

If the server requires a valid email account, you will need to create one for Session Monitor. Then, select **Enable authentication** check box and enter the credentials.

Setting Up the Email Notifications

You can choose how the emails from Session Monitor will look like in the users' mailboxes. The field **Mail sender** is the email address Session Monitor will use; users will see this address in the **Sender:** or **From:** field of the emails. You can optionally specify a **Subject prefix** ; which appears at the beginning of the subject of the emails and make it easy to identify Session Monitor's emails in users' inbox.

Configuring the Capture Settings

The Capture Settings page contains a list of configured network interfaces, with a toolbar for deleting interfaces, as well as a restore button to reset the last applied settings (usually, you want to add interfaces you didn't add during the installation procedure).

There's also a check box below the network list that can be checked if you wish to apply capture settings that won't allow you to reconnect to the Platform Setup Application again.

The following figure shows the Capture Settings page.

Figure 4-7   Capture Settings

> **Note:**
>
> Monitoring is only enabled for machines that are configured as probes. On other machines, the monitoring check box is grayed out.
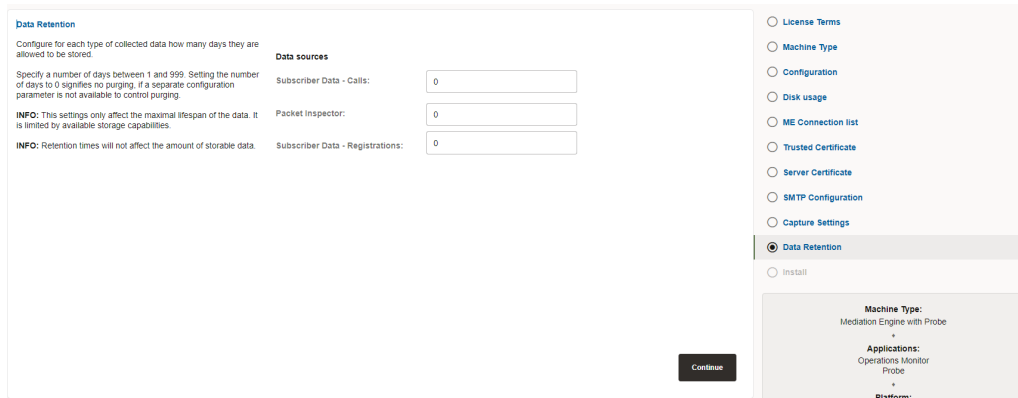
> **Important:**
>
> Do not configure dummy interfaces with DHCP if there is no DHCP server to give an IP. When applying settings with a dummy interface using the DHCP method wait for the DHCP client to time out (usually one minute).

Configuring Data Retention

The Data Retention page is used for configuring data retention in database for different data sources. Some settings depend on the license settings and will be available only if the associated configuration is set.

The following figure shows the Data Retention page.

Figure 4-8   Data Retention page

Data retention is configured in days per data source. A value of 0 disables time based data retention.

> **Note:**
>
> The settings only affect the maximal lifespan of the data. Data availability is limited by available storage capabilities.

> **Note:**
>
> Retention times does not affect the amount of storable data.

You can configure data retention times for the following data sources:

- **CPM Subscriber Data:** Specifies the number of days to consider for storing the Diameter S6 transaction data. Enabled by the CPM module.

- **Media Recording:** Specifies the number of days to consider for storing the RTP recordings. Enabled by RTP recording configuration.

- **Packet Inspector:** Specifies the number of days to consider for storing the network-traffic history. Enabled by Packet Inspector configuration.

- **Subscriber Data - Calls:** Specifies the number of days to consider for storing the call meta data and signaling.

> **Note:**
>
> Saved calls are not deleted by this option. Saved calls must be deleted by operators. (Optional) Disable user permissions for saved call functionality.

- **Subscriber Data - Registration:**Specifies the number of days to consider for storing the registration events.

> **Note:**
>
> CDR/MDRs are not supported. Data retention affects data in the database only. For deleting CDR/MDRs, use FTP to delete files after downloading.

Secure Configuration

To help protect users of Session Monitor and consumers' data, see the Session Monitor Security Guide for information on the security features of Session Monitor.

During the installation of a Session Monitor server, you will encounter the server certificate and trusted certificate pages.

Server Certificate

The Server Certificate page is used to see and change the certificate used by this server. This step is recommended to protect users' data.

For more information, see the discussion about encryption and certificates in the Session Monitor Security Guide.

Installing the Products

The Install page summarizes the components to install. Check that you selected the correct components; after the installation is complete, the selection of the components cannot be changed.

The following figure shows the Install page.

Figure 4-9   Install page
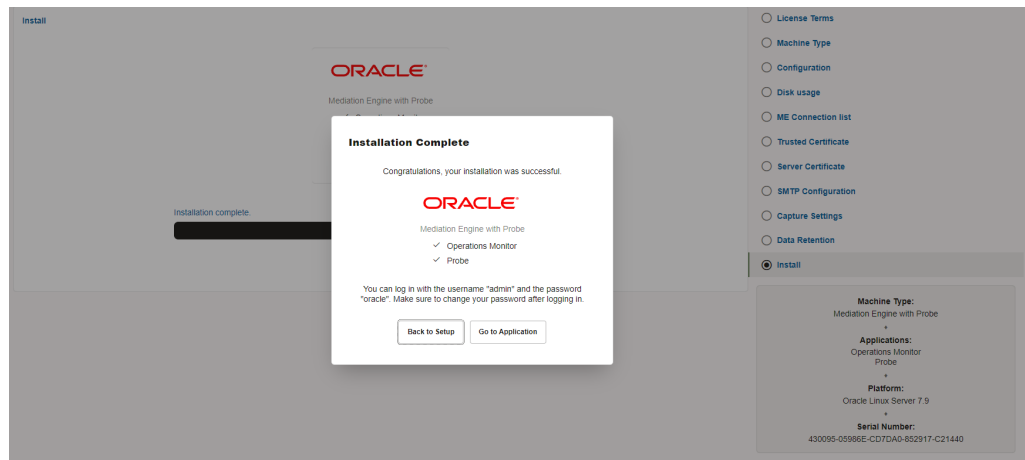
Click **Install** to start with the installation. The Platform Setup Application initiates the installation process and reports back the progress. The installation process might take a few minutes to complete.

You can click on the **Session Monitor** button when the installation is complete. This will bring you to the installed products' interface.

5

Session Monitor Post-Installation Tasks

This chapter provides instructions for Oracle Communications Session Monitor post-installation tasks.

Installing Software Update

After you log in to the product interface, you can see the status of the system or update the system. A system update will update all applications as well as the Platform Setup Application itself.

The Software Version page shows the currently installed components and the software version.

To install a software update, go to the Software Version page and select the update file (file type .rpm) that was provided by Oracle or your service provider. Click **Apply** to initiate the upload.

When the upload has finished, the page will show the version number and issue the date of the update. Click **Install** to proceed with upgrading the system. You can also abort the upgrade by clicking **Clear**.

> **⊘ Important:**
>
> Session Monitor or parts of it may not be available during the update process.

Platform Setup Application will show the progress during the upgrade. You may click **Close** to hide the progress window.

After the successful upgrade, establish an SSH session with the product and execute the following command:

```
source /opt/oracle/ocsm/ocsm_env.sh
```

> **✎ Note:**
>
> If you have a setup with multiple servers (for example, ME, MEC, Probe(s) and OCFM), upgrade all of them at the same time. Running different servers (ME, MEC, probe(s), OCFM) of the Session Monitor on different versions is not supported.

Upgrading the MySQL Version

OCSM Release 5.1 supports upgrade from MySQL 5.7.35 (or higher version of 5.7) to MySQL 8.0.32.

The MySQL upgrade will happen as part of the upgrade to OCSM 5.1. For information on upgrading to OCSM 5.1, see the section Upgrading MySQL section in the Session Monitor 5.1 Upgrade Guide. An upgrade of MySQL 8.0.32 to a newer version will not be available at the time OCSM 5.1 Release as this cannot be verified in our lab. The detailed steps will be made available along with subsequent patches. For more information, contact Oracle Support for further information.

Media Protocols

The Media Protocols menu is available after the installation process has finished and only for machine type Probe (which includes the machine type Mediation Engine with Probe).

You use the Media Protocols page to identify the RTP traffic that the Probe looks for. The Probe accepts only the traffic that matches the BPF filter.

Filters

You can set the media protocols filter as follows:

*   **Check all traffic for signaling:** When this check box is enabled, all traffic (including the traffic that matches the BPF filter rule) is passed to the signaling probes for filtering using the signaling protocols filters. When this check box is disabled, only the traffic that does not match the BPF filter rule is passed to the signaling probes. If you use Packet Inspector for media recording, you need to enable this option to filter the media packets using the Packet Inspector filter in **Signaling Protocols**.

    > ✎ **Note:**
    >
    > Packet Inspector supports STCP, TCP, and UDP as transport protocol for capturing the signaling network traffic or media. Due to the design limitation, other transport protocols such as ICMP are not supported. Enabling this option may decrease system performance.

*   **BPF filter:** This filter identifies the RTP traffic. Only the traffic that matches this filter rule is considered. You might want to configure the filter rule to pick up only the packets you are interested in. Ignoring the unwanted packets reduces the stress on the system and increases performance. The traffic that does not match this filter is passed to the signaling probes for filtering using the signaling protocols filters

See the Signaling Protocols section for more information about signaling protocols.

See the Filter Syntax section for more information about filters.

Status

The following status are shown for the RTP packets:

*   **Active streams:** Specifies the number of RTP streams found. Only the traffic that matches the filter is counted.

- **Packets processed:** Specifies the packets that match the filter and processed successfully.
- **Packets dropped:** Specifies the packets that match the filter but not processed due to insufficient resources.

Signaling Protocols

The Signaling Protocols menu is available after the installation process has finished and only for machine type Probe (which includes the machine type Mediation Engine with Probe).

You use the Signaling Protocols page to identify the types of traffic the various probes (which sniff traffic) look for. The Probe accepts only the traffic that matches the filter rule and sends them to the Mediation Engine.

You might want to configure strict filtering rules for several reasons:

- The probes process all traffic that matches the filter. For most installations, the high volume of traffic makes inspecting every packet infeasible. Ignoring unnecessary packets, therefore, puts less stress on your system and makes subsequent analysis easier. For example, you may want to make sure the signaling probe, which monitors SIP, does not also get all the RTP traffic.
- You might not be interested in certain sources of traffic, even though the machine would pick it up.
- More complex VLAN configurations.

The default filters are sufficient for most installations and provide a good starting point.

After you configure the filters, it takes a few seconds for the probe(s) to reconfigure. The statistics on this page should show the totals for the new filters. The **Packets processed** statistic is a good indicator of how the filters are working.

> **Note:**
>
> - Make sure to use vlan keywords in the filters when that is used on the network.
> - Make sure to change the default filters if you use non-standard ports or other options.
> - Traffic is first filtered using the media protocols setting. Only the traffic that does not match the media protocols BPF filter (except when **Check all traffic for signaling** filter option is enabled) is passed to the signaling probes.
> - If you use Packet Inspector for recording media, you need to include media packets in the Packet Inspector filter.
> - You need to ensure that there is sufficient disk space for storing media on the Probe machine. Media packets are initially stored on the Probe machine. The Probe forwards the packets to the Mediation Engine only when a user downloads the media to a PCAP file. When the disk is full, the Probe overwrites the calls stored on the disk with new calls. You can define the Packet Inspector filter to restrict the calls stored on the Probe and thus minimize calls that are overwritten.

For more information about filters, see the Filter Syntax section.

Packet Deduplication

You can select to turn on packet deduplication for the associated traffic type. If you turn on packet deduplication, you must also provide a time value in milliseconds. The value should be greater than zero.

Packet deduplication is done at L3 and above and it is best effort. Some types of traffic might not get deduplicated, for example, duplicates on nested VLANs, ipv6, and so on.

There is a System Setting to enable deduplication in the core, which should be enabled if there are multiple Probes connected to one ME, and seeing the same traffic. If traffic is seen without and with vlan tags, you should also disable VLAN awareness in **System Setting**.

Statistics per Protocol

The following statistics are shown for each protocol:

- **Rate:** Specifies the total number of packets accepted after the filtering.
- **Packets processed:** Specifies the number of packets processed in the last second. Only packets that match the filter are processed.

Global Statistics

The following statistics are shown for all devices:

- **Total sniffed:** Specifies the number of packets sniffed across all configured devices.
- **Total dropped:** Specifies the number of packets that were not processed. Packets were dropped either by the NICs or during processing due to system performance reasons. If possible, tighten the filter rules and disable the **Check all traffic for signaling**filter option in **Media Protocols** to ignore unnecessary packets and reduce stress on the system. If that is not possible, consider upgrading the machine.

System Diagnostics

The System Diagnostics menu allows the creation of a report with information on the installation. This report may be requested by the support team in case of issues.

Creating a Report

A report can be created by clicking **Create**. This may take several minutes to complete. Afterwards, the report can be downloaded as a file by clicking **Download**. This file can then be sent to the support team, for example by email.

If a report exists, its creation date will be shown. It can be downloaded as often as necessary, but there can be only one report at a time; creating a new report will overwrite any existing one.

Reports are deleted around midnight UTC.

Report Contents

The contents of a report include:

- Information on the available hardware of the machine that the monitoring solution is running on

- Log files

- Configuration of the monitoring solution

- Statistics about the performance and status of components of the system and of the monitoring solution

- If the check box **Include mysql dump...** is checked, the report includes a dump of most of the database tables. Note that the respective tables might be huge.

- If the check box **Include mysql dump...** is not checked, the report will include only minimal information about the database tables.

> ✎ **Note:**
>
> Sensitive information is removed before report creation, including, but not limited to, passwords, keys, and certificates.

Filter Syntax

The filter syntax used is the same as tcpdump or libpcap. For an example, see https://wiki.wireshark.org/CaptureFilters.

The following filters are also known as BPF filters:

- (tcp port 5060)

- ((udp or tcp) and port 5060)

- (vlan (udp or tcp) and port 5060)

- (tcp portrange 5060-5070)

- (not port 5060)

- (host 10.10.0.5 and port 5060)

- (not host 10.10.0.5 and port 5060)

- (not ether dst 12:34:56:78:90:ab)

Entries with a vlan keyword must be included for networks using VLANs. It is harmless to include them on networks which don't use VLANs, but do make sure there is a separate identical filter without the vlan. For example, (tcp port 5060) or (vlan and tcp port 5060).

Support for Backup and Restore

Session Monitor enables you to back up the Configuration, Database, Block Storage, and Potential Customized Files of OCSM Servers using the Backup and Restore procedure.

If you want to reinstall OCSM 5.1 Machine without losing exisiting OCSM 5.1 data, use the OCSM Backup and Restore procedure.

You can use the Backup and Restore procedure back up your older OCSM Release during the upgrade to version 5.1 and restore it if the upgrade fails. For more information, see the Session Monitor Release 5.1 Backup and Restore Guide.

6
Installing and Configuring DPDK for Session Monitor

This chapter provides instructions for installing and configuring Data Plane Development Kit (DPDK) for the Oracle Communications Session Monitor to monitor high volume of network traffic.

DPDK provides sniffing performance for some of the Intel network cards and network traffic patterns. If you have a compatible network card, you can enable DPDK.

> **Note:**
>
> See Oracle Communications Session Monitor Release Notes to verify if you need to update DPDK. If you need to update DPDK, verify if the DPDK requires latest Oracle Linux Platform.

DPDK is a special architecture supported by specific network card designs, drivers, and server architectures, that improves performance when processing network traffic. For high network traffic monitoring, you can select to enable DPDK option on Session Monitor Probes. DPDK uses NUMA architecture special feature to have faster access to traffic written from a Network Card and to enhance the performance.

DPDK architecture involves two parts for Session Monitor Probes. The daemon is responsible for network traffic analysis (rat) is compiled against a specific DPDK library, and is deployed upon Session Monitor installation. For DPDK to work, the DPDK driver must be downloaded and installed on the Probe, as well.

> **Note:**
>
> To install DPDK on a SELinux enabled machine, disable SELinux first and install DPDK. Enable SELinux after the installation of DPDK.

System Requirements

The following sections describe the hardware and software requirements for installing and configuring DPDK for Session Monitor.

> **Note:**
>
> The software and hardware details mentioned in this section are minimum requirements to enable DPDK for capturing high volume of network traffic. Contact Oracle Support for more assistance.

Hardware Requirements

This section describes the hardware requirements for installing and configuring DPDK.

Minimal Requirements

Following are the list of minimum hardware requirements:

- Probe machine (with DPDK) (2 Intel processors, each with 8 cores, 8 GB RAM, Intel based network card)
- Mediation Engine and Probe in one machine (at least 2 Intel processors and 24 cores in total, 24 GB RAM, Intel based network card)

Supported Servers

For supported servers, see the Session Monitor System Requirements section.

Supported Networking Cards

The following networking cards are supported:

- Sun Dual Port 10 GbE PCIe 2.0 Networking Card with Intel 82599 10 GbE Controller
- Sun Quad Port GbE PCIe 2.0 Low Profile Adapter, UTP
- Sun Dual Port GbE PCIe 2.0 Low Profile Adapter, MMF
- Mellanox ConnectX-5 EN network interface card, 100GbE dual-port QSFP28, PCIe3.0 x16, tall bracket

Software Requirements

Supported DPDK versions for Session Monitor

The following table lists the supported versions of DPDK.

Table 6-1   Table 5-1 DPDK Support Versions for Session Monitor

DPDK Version	Session Monitor Release
16.07	Supported from 3.4.0.0.0
18.11	Supported from 4.2.0.0.0
19.08	Supported from 4.3.0.0.0
19.11	Supported from 4.4.0.0.0
21.11.2	Supported from 5.1.0.0.0

Installing and Configuring DPDK with Internet

This section describes the procedure for installing and configuring DPDK for session monitor.

> **Note:**
>
> You must be connected to the internet before starting the installation. Running the following command installs, downloads the required files, and configures the DPDK automatically.

For DPDK installation, for Oracle X9-2 server has the following pre-requisite:

1. Log into the Platform Setup Application page:

   a. Select **Capture Settings**.

   b. Check the box in **Monitoring** column against each sniffing interface that you want to use for capturing the traffic.

2. Log into the machine that hosts the probe or mediation engine and probe as a **root** user.

3. (Optional) For better understanding of the network, CPU, and NUMA nodes of the server, you can run the following command to review the output of the **system_layout.py** script, that will display system information:

   ```
   source /opt/oracle/ocsm/ocsm_env.sh
   /opt/oracle/ocsm/usr/share/pld/rat/system_layout.py
   ```

4. Run the following commands which guides you through the installation:

   ```
   source /opt/oracle/ocsm/ocsm_env.sh
   python3 -m pip install meson
   python3 -m pip install ninja
   python3 -m pip install pyelftools
   yum install -y git
   yum install -y gcc-toolset-11.x86_64
   git clone http://dpdk.org/git/dpdk-kmods (Execute this command in the
   root folder)
   scl enable gcc-toolset-11 '/opt/oracle/ocsm/usr/share/pld/rat/
   configure_dpdk.py'
   ```

   The **configure_dpdk.py** script downloads and installs the required DPDK driver, the corresponding Kernel headers required for compiling DPDK driver, compiles, installs the driver, and creates server and Session Monitor DPDK related configuration.

5. (Optional) To view all the available advanced options, run the following command:

   ```
   /opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py -h
   ```

6. Reboot the machine that hosts the probe or mediation engine and probe.

Installing and Configuring DPDK without Internet

DPDK can be installed and configured without an internet connection.

1. Log into the Platform Setup Application page:

   a. Select **Capture Settings**.

   b. Check the box in Monitoring column against each sniffing interface that you want to use for capturing the traffic.

2. Log into the machine that hosts the probe or mediation engine and probe as a **root** user.

3. (Optional) For better understanding of the network, CPU, and NUMA nodes of the server, run the system_layout.py script to display system information.

   ```
   source /opt/oracle/ocsm/ocsm_env.sh
   /opt/oracle/ocsm/usr/share/pld/rat/system_layout.py
   ```

4. Run the following command to download the Kernel:

   > **✎ Note:**
   >
   > For offline installation of DPDK, check the Kernel version before downloading. The Kernel version in the `Download_rpms.sh` script is currently - "`kernel-uek-devel-5.15.0-3.60.5.1.el8uek.x86_64.rpm`". The Kernel dependency libraries are also present in the `Download_rpms.sh` script. The Kernel version is subject to change and hence we recommend you to check the `uname -r` and then download the corresponding RPM file and their dependencies from the YUM repository and place the appropriate Kernel version RPM file in the `Download_rpms.sh script`. Or, you can download and copy the RPM file and their dependencies to the existing offline REPO server. For more information, see Installing Session Monitor Offline.

5. After downloading the RPM file, run this command to install the Kernel.

   ```
   yum install kernel-uek-devel-$(uname -r)
   ```

6. Download the DPDK tar.gz file from https://fast.dpdk.org/rel into the folder `/var/cache/ocsm/dpdk/`.

7. Run the below commands on a linux terminal connected to internet and download the `dpdk-kmods` folder:

   ```
   yum install git
   git clone http://dpdk.org/git/dpdk-kmods
   ```

8. Copy the downloaded `dpdk-kmods` folder into **root** of the system where DPDK needs to be installed.

9. Download the latest `.whl` files for the meson, ninja and pyelftools libraries from the URLs mentioned below:

Table 6-2   Download URLs

Item	URL
meson-X.X.X-py3-none-any.whl	https://pypi.org/project/meson/#files
ninja-1.11.1-py2.py3-none-manylinux_X_XX_x86_64.manylinux20XX_x86_64.whl	https://pypi.org/project/ninja/#files
pyelftools-X.XX-py2.py3-none-any.whl	https://pypi.org/project/pyelftools/#files

10. Run the following commands as a **root** user:

```
source /opt/oracle/ocsm/ocsm_env.sh
pip3 install meson-X.X.X-py3-none-any.whl --no-index
pip3 install ninja-1.11.1-py2.py3-none-
manylinux_X_XX_x86_64.manylinux20XX_x86_64.whl --no-index
pip3 install pyelftools-X.XX-py2.py3-none-any.whl --no-
index
yum install -y gcc-toolset-11.x86_64
scl enable gcc-toolset-11 '/opt/oracle/ocsm/usr/share/pld/rat/
configure_dpdk.py'
```

11. (Optional) To view all the available advanced options, run the following command:

```
/opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py -h
```

12. Reboot the machine that hosts the probe or mediation engine and probe.

Updating DPDK

This section provides the instructions to update DPDK after a Kernel update.

> **Note:**
>
> You must perform the instructions in this section if you have installed another Linux Kernel.

To update DPDK:

1. Reboot the system.

2. Follow the procedure detailed in Installing and Configuring DPDK with Internet or Installing and Configuring DPDK without Internet depending on your setup. For MLNX NIC cards following instructions Installing and Configuring DPDK for Mellanox NIC Cards.

3. Reboot the machine that hosts the probe or mediation engine and probe.

DPDK with Higher Throughput

Starting with OCSM Release-5.1.0.0.0, both dynamic memory mode and legacy memory mode is supported. DPDK probe can reach up to 3.2 Mpps on a single port when legacy memory mode is enabled.

> **Note:**
>
> This applies only for Intel NIC cards.

Legacy Memory Mode

Add the below configurations in the `rat.dpdk.local.conf.`

```
[dpdk]
mem_mode = 2

[sniffer/xx_xx_x]
dpdk_rx_ring_desc = 1024
```

After making the changes, restart the rat process using the command `systemctl restart pld-rat`.

Uninstalling DPDK

This section describes the instructions for uninstalling DPDK.
To uninstall DPDK:

1. Run the following commands:

    ```
    source /opt/oracle/ocsm/ocsm_env.sh

    /opt/oracle/ocsm/usr/share/pld/rat/configure_dpdk.py --remove
    ```

2. Reboot the machine that hosts the probe or mediation engine and probe.

7

Downloading, Installing, and Configuring DPDK for Mellanox NIC Cards

Follow the instructions in this section to install and configure DPDK for Mellanox NIC cards.

1. Installing Mellanox OFED
2. Installing and Configuring DPDK

Installing Mellanox OFED

Complete the following tasks to download and install Mellanox OFED package for Oracle Linux.

The supported networking cards are: Mellanox Technologies MT27800 Family [ConnectX-5].

Ensure that you have installed:

- Oracle Linux 8.6
- Session Monitor 5.1
- DPDK Version 21.11.2 or higher.

1. Download the latest MLNX OFED driver (.iso) based on OS distribution and architecture from the MLNX_OFED Download Center page. Browse to **Downloads** - > **Current Versions**.

> ✎ **Note:**
>
> The drivers MLNX_OFED latest support is available till OL8.6. The drivers are not available for OL8.7 and supports only OL8.6

2. Run the commands:

   a.
   ```
   mount -o ro,loop MLNX_OFED_LINUX-xxxx /mnt
   ```

   b. Run this command:

   ```
   yum install rpm-build
   ```

> **Note:**
>
> The command may fail while building RPMs and may require the appropriate dependencies to be installed. Based on the dependency errors, the required packages must be installed.
> This would build the RPMs based on the underlying Kernel version and copy the RPMs to `/tmp/xxx.tgz`.

c.

```
cd /mnt/
/mnt/mlnx_add_kernel_support.sh -m /mnt --make-tgz
```

3. Install the MLNX OFED with upstream-libs:

```
cd /tmp
tar -xzvf MLxxxxx.tgz
cd /MLxxxxxxxx
./mlnxofedinstall --upstream-libs
```

> **Note:**
>
> For more information, see Installing Mellanox OFED.

4. Load the MLNX driver module.

```
modprobe mlx5_ib
```

5. Make sure that the `mlx kernel modules mlx5_ib`, `mlx5_core`, `ib_uverbs` are loaded.

```
lsmod | grep mlx5
lsmod | grep ib_uverbs
```

Installing and Configuring DPDK

Complete the following tasks to install and configure DPDK for Mellanox NIC cards.

1. Create a file `/opt/oracle/ocsm/etc/iptego/white_list_dpdk.local` with the value **mlx5_core** before starting the DPDK installation.

2. Log into the **Platform Setup** Application page.

   a. Select **Capture Settings**.

   b. Check the box in the **Monitoring** column against each sniffing interface that you want to use for capturing the traffic.

3. Log into the machine that hosts the probe or the mediation engine and probe as a **root** user.

(Optional) For better understanding of the network, CPU, and NUMA nodes of the server, run the `system_layout.py` script to display system information.

```
source /opt/oracle/ocsm/ocsm_env.sh
/opt/oracle/ocsm/usr/share/pld/rat/system_layout.py
```

> **Note:**
>
> If you observe a Python error while executing the .py files, run the command `update-alternatives --config python3` and select the `/usr/bin/python3.9` option.

4. Run the command:

```
yum install kernel-uek-devel-$(uname -r)
```

5. Download the DPDK tar file from https://fast.dpdk.org/rel/ into the folder `/var/cache/ocsm/dpdk/`.

6. Untar and open the file in edit mode.

```
/var/cache/ocsm/dpdk/dpdk-<version>/config/common_base
```

7. Run the following commands as a root user:

```
source /opt/oracle/ocsm/ocsm_env.sh
python3 -m pip install meson
python3 -m pip install ninja
python3 -m pip install pyelftools
yum  install gcc-toolset-11.x86_64
scl enable gcc-toolset-11 '/opt/oracle/ocsm/usr/share/pld/rat/
configure_dpdk_mlx.py'
```

8. Reboot the machine that hosts the probe or the mediation engine and probe.

9. MLNX drivers require root privileges for the Promiscuous Mode to be enabled. Assign **root** user privileges to the **ocsm** user.

10. Open file in edit mode: `/etc/passwd`

11. Change line `ocsm:x:998:996::/opt/oracle/ocsm:/sbin/nologin` to `ocsm:x:0:0::/opt/oracle/ocsm:/sbin/nologin`

12. Restart the RAT service (pld-rat): `systemctl restart pld-rat`

8

Installing Skype for Business Agent

This chapter explains how to install the Skype for Business Agent for Oracle Communications Enterprise Operations Monitor, and Oracle Communications Operations Monitor.

Overview

For Enterprise Operations Monitor (EOM) to monitor Skype for Business encrypted SIP messages, the user must install a Windows service (Agent) on the Skype for Business server. The Skype for Business Agent registers itself on the server and acts as a back-to-back user agent for the Skype for Business calls, obtaining access to the SIP message bodies. It then forwards the SIP messages to the EOM Mediation Engine, which analyzes them and displays them in the calls list alongside regular VoIP calls.

The Skype for Business Agent is distributed as a regular Windows .msi package which offers a wizard based installation.

Pre-requisites

Before installing Skype for Business Agent, ensure that you have the following:

- Mediation Engine is installed on Linux and the Skype for Business Server machine is able to connect to the Mediation Engine.

Installing Skype for Business Agent

To install Skype for Business Agent:

1. Download the Skype for Business installation file to a temporary directory (temp_dir).
2. Go to the *temp_dir* directory.
3. Unpack the **Skype for Business to Skype Agent** for Business (SFB) server.
4. Run the **Skype for Business Agent** file.

   The Oracle EOM Skype for Business Agent Setup wizard appears.
5. Click **Next**. The End-User License Agreement screen appears.
6. Accept the license agreement and click **Next**.

   The ME Connection Settings screen appears.
7. In the **ME Host Address** field, enter host address.
8. It is recommended not to deselect **Use TLS**. When selected, the connection to Mediation Engine is encrypted.

> **Note:**
>
> If encryption is selected, you must generate a TLS certificate for the Skype for Business Agent which includes a Certificate. Upload the TLS certificate to the Enterprise Operations Monitor machine, and install it on the Skype Server in the local computer Trusted Certification Authorities store, and install the generated certificate including the private key permissions in the Personal Certificate store.

> **Note:**
>
> **Important:**
>
> •   Grant the read permissions for the private key to the OracleSkypeProbeUser account.
>
> •   If encryption is not selected, the user must also select the Allow insecure connection checkbox in the Trusted certificates section in the Enterprise Operations Monitor setup.

The Ready to Install Oracle EOM Skype Agent screen appears.

9.   Click **Install**.

The installation sets up a service on the windows server and creates an user account,**OracleSkypeProbeUser** for the service.

10.   Click **Finish**.

The Skype for Business Agent installation is now complete and the calls made from Skype will appears as a Skype call in the call details window.

Uninstalling Skype for Business Agent

To uninstall Skype for Business Agent:

1.   From your machine, click **Start** and then click **Control Panel**.

2.   Click **Programs**.

3.   Click **Program and Features**.

4.   In the list of currently installed programs, select **Oracle EOM Skype for Business Agent** and then click **Uninstall/Change**.

5.   A confirmation dialogue box appears. Confirm Uninstallation.

The Skype for Business Agent is uninstalled.

Editing ME Host Address

To edit the ME host address:

1.   Open the configuration file, **C:\Program Files\Oracle\Oracle EOM> Skype Probe\SkypeProbe.exe.config.**

2. Change the value of the tag having key, **apidAddr**.

   For example:

   ```
   <add key="apidAddr" value="192.168.123.120"/>
   ```

3. Save the **SkypeProbe.exe.config** file.

4. Place the cursor on the **Oracle EOM Skype Probe** service name and right click to restart.

Configuring Skype for Business Agent for Monitoring Call Quality Information

The Skype for Business Agent monitors only the SIP call flow. The call quality information is reported by the user agent, Skype for Business Desktop Client.

To get the call quality information:

1. Enable monitoring on the Skype server.

   See https://docs.microsoft.com/en-us/skypeforbusiness/deploy/deploy-monitoring/deploy-monitoring.

2. Install and configure the Skype for Business SDN API on the Skype Front-End Server, as described in the Skype for Business SDN API 2.4.1 Installation Admin Guide.

   See https://docs.microsoft.com/en-us/skype-sdk/sdn/articles/installing-sdn-interface.

3. After the installation, add the Mediation Engine machine to Skype for Business Server as a subscriber for the SDN API by running the following command in the Skype for Business Server console:

   ```
   SDNManager.exe /p s EOM submituri=https://<IP_address>/sfb/
   ```

   where *<IP_address>* is the IP address or the hostname of your Mediation Engine.

   The finished Skype calls show the MOS values and media summary.

4. Configure the SDN Manager to send QualityUpdate messages to the Mediation Engine by running the following command:

   ```
   SDNManager.exe /p s EOM "quality=True"
   ```

5. Operations Monitor reads the SDN Interface messages from the URL https://<Mediation Engine Host>/sfb/.

   ```
   cd "C:\Program Files\Microsoft Skype for Business
   Server\Microsoft Skype for Business SDN Manager\"
   SDNManager.exe /parameter subscriber ocom "submituri=https://
   <MediationEngine Host>/sfb/"
   ```

6. After configuring the SDN Dialog Listener and SDN Manager, run the following command for SDN Manager to forward the messages to Operations Monitor:

   ```
   cd "C:\Program Files\Microsoft Skype for Business Server\Microsoft Skype
   for Business SDN Manager\"
   ```

```
SDNManager.exe /parameter subscriber ocom "submituri=https://
<MediationEngineHost>/sfb/"
```

7. Verify the SDN Manager configuration:

```
cd "C:\Program Files\Microsoft Skype for Business Server\Microsoft
Skype for Business SDN Manager\"
SDNManager.exe /download subscriber
```

You should get an XML describing the configuration.

> **✎ Note:**
>
> Make sure the value of the submituri parameter matches the address of the Enterprise Operations Monitor machine.

8. Check the SDN Manager and Dialog Listener log files at `%LOCALAPPDATA%`
   `\Local\Temp\SDN` after each Skype for Business call. Open the
   `SDNManager.log` file and search for the following:

```
Starting to transmit the message?
```

If the line does not exist, the SDN manager is configured incorrectly. Repeat the configuration process again.

Troubleshooting

This section provides guidelines for troubleshooting problems with Skype for Business Agent.

Problems with Viewing Skype Call Data Information

Perform the following if you are unable to view skype call data:

1. Verify that the **SkypeProbe.exe.config** file located in the installation directory has the correct IP address of Mediation Engine.

2. Verify Mediation Engine machine is reachable by pinging the Mediation Engine Machine from Skype for Business Server.

3. Verify the logs for any exceptions or connection errors in the following path:

   C:\ProgramData\Oracle EOM Skype Probe\Logs

4. Ensure that **OracleSkypeProbeUser** is a member of RTC Server Applications local group. If not, add the user by doing the following:

   a. From your computer, click **Start** and search for **Computer Management**.

   b. Click **Computer Management**.

   The Computer Management screen appears.

   c. Click **Local Users and Groups**.

    d. Select and right-click the **RTC Server Applications** group and click **Add to Group**.

    e. Locate and add the **OracleSkypeProbeUser** and click **OK**.

      The **OracleSkypeProbeUser** will be added to the RTC Server Applications group.

5. Verify the Enterprise Operations Monitor Skype for Business agent service is running in services.msc. by doing the following:

    a. From your computer, click **Start** and search for **Computer Management**.

    b. Click **Computer Management**.

      The Computer Management screen appears.

    c. Click **Services and Applications**.

    d. Click **Services**.

    e. Verify if Skype for Business Agent service is running, if not, right-click the service and click **Start**.

      The Skype for Business Agent will start running.

6. Verify if the connection between Mediation Engine and Skype for Business Server is blocked by firewall. If blocked, disable the setting depending on your Operating System.

7. If you have selected **Accept insecure connections from remote probes** during Enterprise Operations Setup, set the **UseTls** parameter to false in the **SkypeProbe.exe.config** file.

9

Public Cloud Platforms

You can run Oracle Communications Operations Monitor on the following public cloud platforms:

- OCI
- AWS
- Azure

> **Note:**
>
> Refer to the OCSM 5.1 Release Notes for confirmation on the public clouds supported and important details on the software version's support.

This section addresses requirements associated with running the Operations Monitor as public cloud instances. It also provides basic instructions on deploying machine instances. Public Cloud providers maintain extensive product documentation. You must use those vendors' documentation for specifications, requirements, caveats, known issues, deployment details, and operation details prior to deploying the OCSM.

Create and Deploy OCSM on OCI

You can deploy the Mediation Engine (ME), FDP, and Mediation Engine Controller (MEC) nodes of the Oracle Communications Session Monitor (OCSM) on Oracle Cloud Infrastructure (OCI). When deployed on the OCI platform, you configure and operate the OCSM as you would on any other platform. You can deploy the OCSM to use the environment's IP infrastructure, including the private and public addressing scheme.

Before installing OCSM components, SSH keys must be generated to access the OCSM VM instances.

For more information, see Generating an SSH Key Pair on Windows Using the PuTTYgen Program.

Deployment Checklist

Before starting the deployment, ensure that you have the following information handy.

Contact the OCI account administrator to assign the required privileges in IAM to create and/or use the following OCI resources:

- Identify and deploy to the correct OCI Region and compartment. This is typically a default component of the OCI Account.
- Identify and deploy to the correct OCI Availability Domain
- Identify and deploy to the correct OCI Fault Domain

- Prepare private and public key. For more information, see Generating an SSH Key Pair on Windows Using the PuTTYgen Program.

- Create Networks and Subnet - The OCI interface types include those hidden from the internet and those that are not. Oracle recommends creating regional subnets, which means the subnet can span across availability domains within the region. Refer to OCI's Regional Subnets documentation for further information about using these objects

- Identify and select or create the appropriate Virtual Cloud Network (VCN). Required VCN configuration includes:

  – Security list— these access control lists provide traffic control at the packet level.

  – Subnet configuration— Select a subnet as required

  – Internet Gateway—create a default internet gateway for the compartment and give it an appropriate name.

  – Route table (Use Default)—create a route table to route appropriate Subnet(s) through the Internet Gateway

Security Objects

Security lists specify the type of traffic allowed on a particular type of subnet.

Rules set on the security lists can be either stateful or stateless. Stateful rules employ connection tracking and have the benefit of not requiring exit rules. However, there is a limit to the number of connections allowed over stateful connections and there is a performance hit. Oracle, therefore, recommends stateless lists for media interfaces.

The security list for management ports can be stateful.

Port Numbers for Importing Traffic
Allow inbound traffic for the following ports.

Port no	Service	Protocol
22	SSH	TCP
111	rpcbind	TCP and UDP
80	Nginx	TCP
443	Nginx	TCP
4739-4742	apid	TCP
161	snmp	TCP and UDP

For more information, see the Oracle Communications Session Monitor Security Guide.

Minimum Recommended Shapes

Identify the shape, the minimum recommended shape is 4 OCPU, 8GB RAM, 80GB hard disk and 2 vNIC.

Table 9-1

Machine	Hardware Configuration	Shape Name in OCI
Mediation Engine (ME)	• 4v CPU • 30 GB RAM • 256 Gib HDD	VM.Standard 2.2
Meditation Enigne Connector (MEC)	• 4v CPU • 30 GB RAM • 100 Gib HDD	VM.Standard 2.2
FDP	• 4v CPU • 30 GB RAM • 200 Gib HDD	VM.Standard 2.2

Deployment on OCI

The OCI instance configuration procedure includes a multi-dialog wizard that presents configuration options in sequence.

1. Login to the OCI console by selecting the appropriate region and compartment.

2. Click **Create a VM instance**.
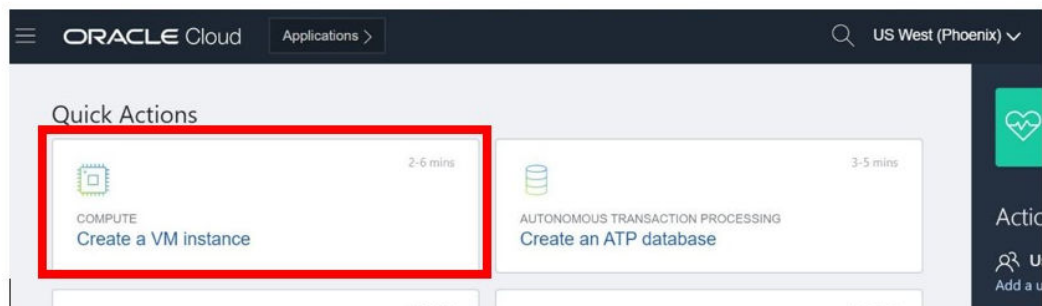
3. In the **Create Compute Instance** page, provide a name for the instance.

    a. Select a compartment from the list of compartments.

    b. Select the appropriate Oracle Linux base image version that is required.

4. Click **Change Shape** to change the Instance shape.

    a. You can choose from two Standard Instance Types: a) Virtual Machine and b) Bare Metal Machine.

    b. Select a Shape. Select one option from the available options - `AMD Rome`, `Intel Skylake`, `Speciality and Legacy`.

    > ✎ **Note:**
    >
    > In the OCSM Release 5.1, OCSM has been tested only with the `Intel` shape.

      c. Select a shape according to your requirement for the Virtual Machine created.

5. Select the **Virtual Cloud Network Compartment**.

6. Select **Virtual Cloud Network**.

7. Select **Subnet Compartment**.

8. Select a subnet as required and choose **Assign a Public IP Address**.

9. In Configure boot volume screen, select **SPECIFY A CUSTOM BOOT VOLUME** and mention the required size.

10. In the **Add SSH keys** screen, choose the appropriate SSH key. Use one option to add the public key: `Generate SSH Key Pair`, `Upload Your Own Public Key`, `Paste own public key`.

11. In the **Show Advanced Options** screen, provide if any details are required.

12. Review the details which are selected or created in the previous steps, make changes if anything is required.

13. Click **Create** to start creating the instance.

14. After a delay of few minutes, the instance is created and the public and private IP addresses of the instance are displayed in the newly loaded page.

15. By default, the instance /(/root) file system has 40 GB only; even if you have defined the size in the earlier step. Follow the method explained in the document How To Create a Linux Instance With Custom Boot Volume and Extend The Root Partition in OCI: to increase the size.

16. After resizing the VM instances, follow the instructions in the Oracle Communications Session Monitor Installation Guide.

> **Note:**
>
> If the disk size is increased after the OCSM installation and configuration, partitions space can be reconfigured by using script:
>
> ```
> /opt/oracle/ocsm/usr/share/pld/scripts/admin/change-disk-usage.py
> ```
>
> For example:. `/opt/oracle/ocsm/usr/share/pld/scripts/admin/change-disk-usage.py -d1 <new-size> -d2 <new size>`
>
> Use d2 only if dual disks are being used. However, if the new partition space is lesser than the previous size then data is deleted. Ensure that the size is larger than the preconfigured size.

Create and Deploy OCSM on Azure

You can deploy the Oracle Communications Operations Monitor on Azure public clouds.

Azure provides multiple ways of managing your environment(s), including via its web portal, using its powershell, and its CLI interfaces. This document focuses on the portal. The portal provides navigation via a web-page pane with links to specified functions on the left side of portal pages. These procedures also assume you have reviewed Azure documentation, and can access portal pages and navigation.

Before beginning, refer to the Oracle Communications Session Monitor 5.1 Release Notes to confirm the public clouds and important details on the software versions supported.

Prerequisites to Azure Deployment

This section addresses requirements associated with running the OCSM in public cloud instances.

The Azure cloud deployment infrastructure provides a flexible management system that allows users to create objects required during the instance deployment procedure prior to or during that deployment. When created prior to deployment, these objects become selectable, typically from drop-down lists in the appropriate deployment dialogs. These objects can be used for a single deployment or for multiple deployments.

The prerequisites for Azure deployment are:

- An account that has the privileges to create or use the resources.
- Azure Subscription details
- Information on the Region
- Resource Group details
- Public and Private subnet.
- Public and private keys. For more information, see Quick Steps - Create and use an SSH public-private key pair for Linux VMs in Azure.

Deploying the Azure Instance

The configuration procedure includes a multi-dialog wizard that presents configuration options in a sequence.

The instance deployment wizard sequence includes:

1. Creating a virtual machine
2. Perfoming disk configuration
3. Configuring networking
4. Management and Configuration
5. Reviewing

Creating a VM Instance for Azure Deployment

Perform the following tasks to create a VM instance.

In the Instance Deployment Wizard, click **Add**, and then click **Virtual Machine**.
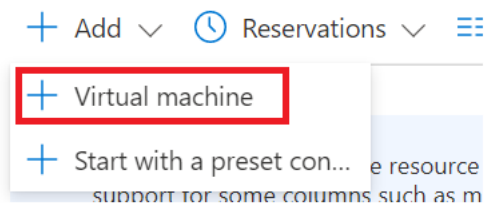
Azure Instance Deployment - Basics Configuration

The Azure instance deployment Basics configuration includes:

- Chose the appropriate subscription and resource group
- Specify the name as your Virtual machine name.
- Select your Region and Availability Option.
- Browse all public and private images and search for Oracle Linux 8.x
- Select the appropriate size of the image, and the minimum recommended shape.

Virtual Machines for Azure Deployment

The table lists the minimum recommended shapes and size for virtual machines to deploy OCSM on Azure.

Table 9-2   VM Shapes and Sizes

Machine	Hardware Configuration	Shape Name in Azure
Mediation Engine (ME)	• 8v CPU • 16 GB RAM • 80 Gib HDD	Standard F8s
Medication Engine Connector (MEC)	• 8v CPU • 16 GB RAM • 80 Gib HDD	Standard F8s
Fraud Monitor (FDP)	• 8v CPU • 16 GB RAM • 80 Gib HDD	Standard F8s

Providing the Administrator Account Information

You can use either of the two methods to sepcify the Administrator Account information.

- Select Authentication Type as **Password**, create a user and assign any password to this user.

- The recommended method is to use the Authentication Type as **SSH public key**.

  – Create a user and provide the SSH public key from the machine you will use to log in to OCSM.

  – During the instantiation, this key is added to the **ssh-key** configuration element as an authorized-key for the user.

Inbound Port Information

Specifying your Inbound port rules external port access to interfaces.

Figure 9-1   Inbound Port

Specifying Disk Options

Disk configuration for Azure Deployment includes setting the OS disk type to Premium SSD for better performance.

Figure 9-2   Disk Configuration

OS disk

OS disk type * ⓘ	Premium SSD (locally-redundant storage) ⌄
Delete with VM ⓘ	☑
Key management ⓘ	Platform-managed key ⌄
Enable Ultra Disk compatibility ⓘ	☐

Network Configuration

Configure networking configuration for your Virtual Machine.

1. Select or create a new Virtual Network.

2. Select or create your Subnet.

3. Enter a name as your Public IP.

4. Select inbound ports (Required).

Figure 9-3   Network Configuration

Completing the Instance Creation

Complete the creation of your instance by retaining the default values.

In the **Management**, **Advanced** and **Tags** tabs, leave the default values as is. You can define tags to clarify details about the instance objects. You do not need to configure anything on the **Tags** tab.

In the **Review and Create** tab, review your settings, and click **Create** to complete instance creation.

The VM instance is ready for OCSM installation. For information on the installation of OCSM components, see Oracle Communications Session Monitor Installation Guide.

Resizing the Root File System

By default, the instance /(/root) file system will have 30 GB only.

If you need to resize the root file system, see Expand an Azure Managed Disk.

Port Numbers for Importing Traffic

Allow inbound traffic for the following ports.

Port no	Service	Protocol
22	SSH	TCP
111	rpcbind	TCP and UDP
80	Nginx	TCP
443	Nginx	TCP
4739-4742	apid	TCP
161	snmp	TCP and UDP

Changing Public and Private IP Address from Dynamic to Static

By default, the Azure VM has a dynamic IP address which changes during the reboot. Hence you need to change from dynamic to static.

1. Click the Public IP address under the **Overview** section.

2. See the accompanying screenshot:

Figure 9-4   Public IP Address
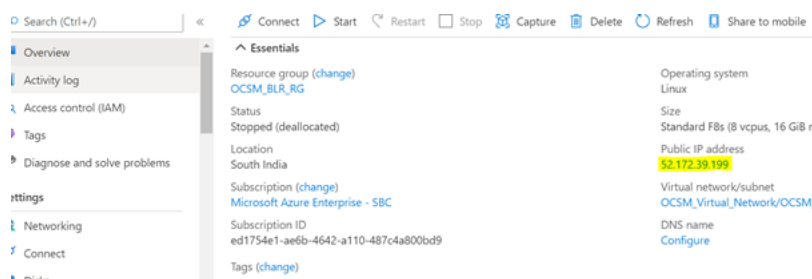
3. Choose Static or Dynamic as per your requirement then click **Save**.

Figure 9-5   Save IP address
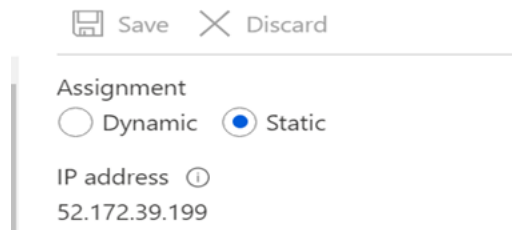
4. Click Networking on the side panel.

5. Click on the network interface as shown in the graphic.

Figure 9-6   Network Interface
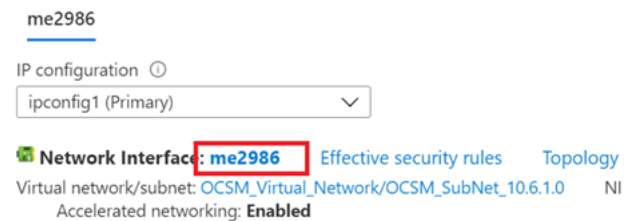
6. Click **Private IP** under **IP Configuration**.

7. Assign the Dynamic or Static IP address.

Figure 9-7   Static and Dynamic Address
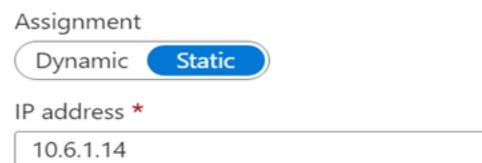
Resizing Disk After OCSM Installation

Perform the following tasks to resize the disk after OCSM Installation.

1. Run the df -kh, verify the added space on the VM.

2. Check the database and UI for the traffic that was run prior to the upgrade. Look for the user and IP address using User Tracking and IP Tracking.

3. Verify that the data exists in **Calls** table. All data present before resize is still available in the system.

4. Verify the size of root partition from the VM system. The disk with the column **Mounted On** which has the **/** value is the root partition. Make a note this value. The size that is displayed is based on the configuration.

5. Verify the disk_quota.conf file values for each partition size. You can find the file under: /opt/oracle/ocsm/etc/iptego/disk_quota.conf.

6. Run the following command to resize the disk space:

```
/opt/oracle/ocsm/usr/share/pld/scripts/admin/change-disk-usage.py -d1
<new-size> -d2 <new size>
```

7. **Note**: Use d2 if dual disks are being used.

8. If the new disk space is lesser than the previous size, then data is deleted. Ensure that the size is larger than the preconfigured size.

9. Disk space is added to the partition as configured. Verify the changes from the file: `cat /opt/oracle/ocsm/etc/iptego/disk_quota.conf`

Create and Deploy OCSM on AWS

This section provides information on the process for creating an AWS VM.

You must use those vendors' documentation for specifications, requirements, caveats, known issues, deployment details, and operation details prior to deploying the OCSM.

Prerequisites for AWS Deployment

The prerequisites for AWS deployment are:

- An account that has the privileges to create or use the resources.
- AWS Account ID and credential details
- Information on the Region
- Resource Group details
- Public and Private subnet.
- Public and private keys. For more information, see Create a key pair using Amazon EC2.

Deploying the AWS Instance

The configuration procedure includes a multi-dialog wizard that presents configuration options in a sequence.

The instance deployment wizard sequence includes the following steps:

1. Creating a virtual machine
2. Preforming disk configuration
3. Configuring networking
4. Management
5. Reviewing configuration

Creating a VM Instance for AWS Deployment

Perform the following tasks to create a VM instance:

1. In the **Instance Deployment** wizard, click **Launch Instances**.

2. Click **Launch Instances**.

Figure 9-8   Launch Instances menu option
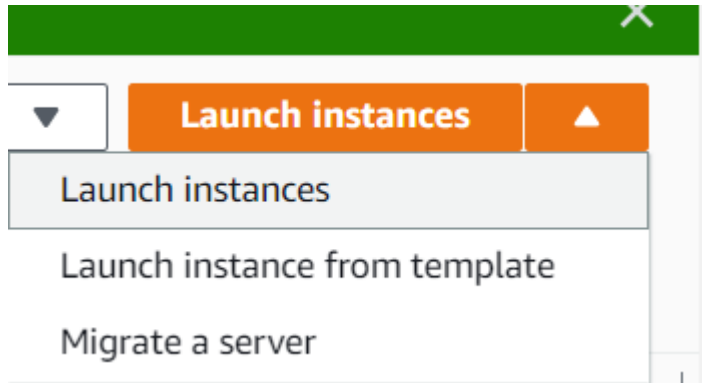
Basics Configuration

The basic configuration for the AWS instance deployment includes:

- Get started by completing the tasks outlined in the **Launch Instances** dialog box.
  - Chose the appropriate region
  - Specify the name as your Virtual machine name
  - Browse all public and private images and search for Oracle Linux 8.6
  - Select the appropriate size of the image, and the minimum recommended shape.

Figure 9-9   Launch an Instance

Security Objects

Security lists specify the type of traffic allowed on a particular type of subnet.

Rules set on the security lists can be either stateful or stateless. Stateful rules employ connection tracking and have the benefit of not requiring exit rules. However, there is a limit to the number of connections allowed over stateful connections and there is a performance hit. Oracle, therefore, recommends stateless lists for media interfaces.

The security list for management ports can be stateful.

Port Numbers for Importing Traffic
Allow inbound traffic for the following ports.

Port no	Service	Protocol
22	SSH	TCP
111	rpcbind	TCP and UDP

Port no	Service	Protocol
80	Nginx	TCP
443	Nginx	TCP
4739-4742	apid	TCP
161	snmp	TCP and UDP

For more information, see the Oracle Communications Session Monitor Security Guide.

Virtual Machines for AWS Deployment

The minimum recommended shapes and size for virtual machines to deploy OCSM on AWS:

Machine	Hardware Configuration	Shape Name in AWS
Fraud Monitor (FDP)	• 16v CPU • 30 GB RAM • 400 Gib HDD	c4.4xlarge
Mediation Engine (ME)	• 16v CPU • 30 GB RAM • 400 Gib HDD	c4.4xlarge
Medication Engine Connector (MEC)	• 16v CPU • 30 GB RAM • 400 Gib HDD	c4.4xlarge

Providing the Administrator Account Information

Use a key-pair to connect to your instance securely. Before you launch the instace, ensure that you have access to the key-pair.

- Select the key pair name created in the previous section. or create a new key pair for the machine you will use to log in to the OCSM instance.

  During the instantiation, this key is added to the SSH-key configuration element as an authorized-key for the user.

Figure 9-10   Select the key pair name
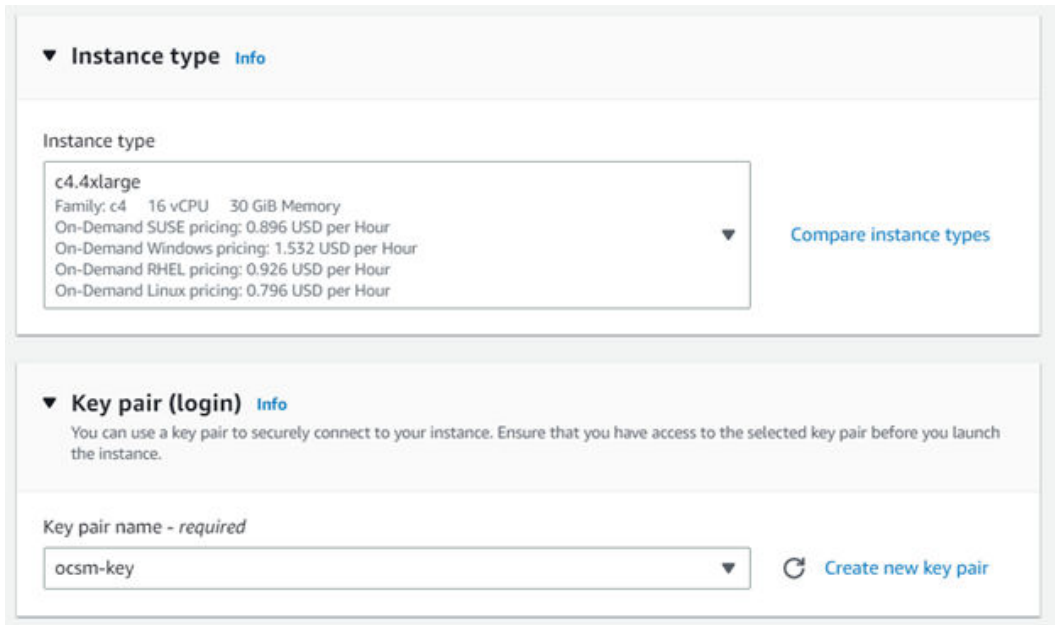
Configuring Network

Configure networking for your Virtual Machine.

- Configure the following networking components for your Virtual Machine:
  - Select or create a new Virtual Network(VPC).
  - Select or create your Subnet.
  - Enter a name as your Public IP.
  - Select or create the security group.

Figure 9-11   Network Settings
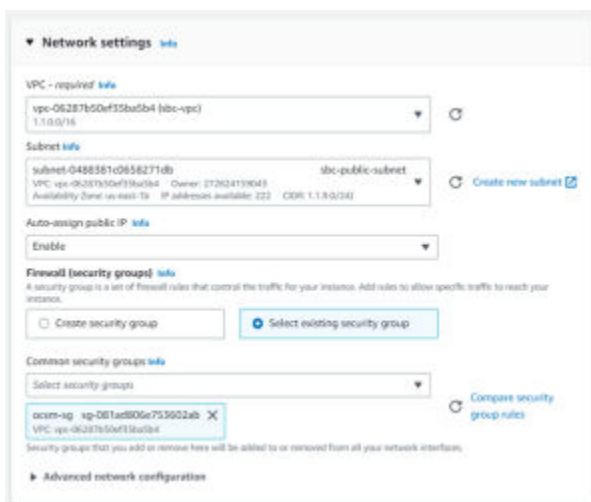
Configure Storage

Disk configuration for AWS Deployment includes setting the OS disk type to SSD for better performance.

- See the Configure Storage screen for information on the values that need to be specified

Figure 9-12   Configure Storage
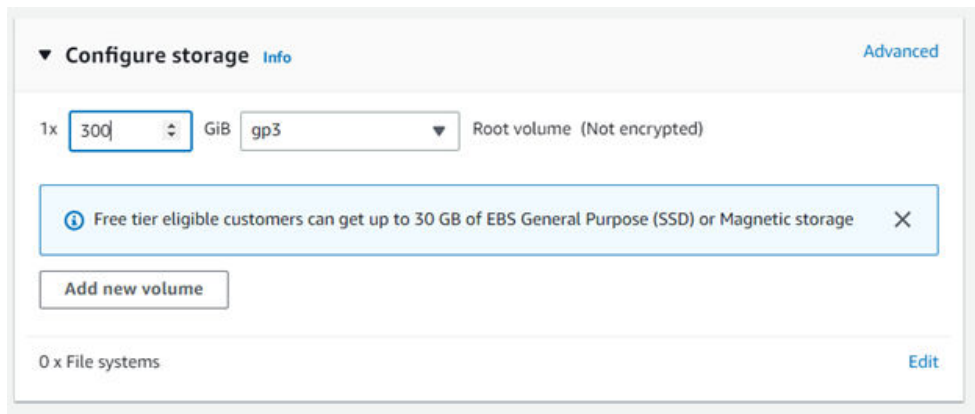
Completing the Instance Creation

Complete the creation of your instance by retaining the default values.

1. In the **Advanced** tab, leave the default values as is.

2. You can define tags to clarify details about the instance objects. You do not need to configure anything on the Tags.

Palladion Ports Usage

This document provides information on port numbers, protocols, and endpoints. This information is meant for the operators deploying OCSM to configure the required firewalls/ACLs.

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME, RM	TCP	80	HTTP	No	Access to Web interface	Any	Random
ME, RM	TCP	443	HTTPS	Yes	access to Web interface	Any	Random
ME, Probes, RM	TCP	22	SSH	Yes	access to CLI interface	Any	Random
ME	TCP	21	FTP	No	access to FTP interface	Any	Random
Probes	TCP	8084-8086	ZMQ	No	RPC server for VQ records of the RTP probes	ME	Random
Probes	TCP	18084-18086	XML-RPC	No	publishers for VQ records of RTP probes	ME	Random
Probes	TCP, UDP	4004 - 4006	ZMQ	No	control interfaces server of RTP probes	ME	Random
Probes	TCP	18000-18020	ZMQ	No	publishers for signaling messages	ME	Random
ME	TCP	5005	ZMQ	No	publisher for RTP streams description	Probes	Random
ME, Probes	UDP	123	NTP	No	time synchrnoization	Time server	123
ME	UDP	53	DNS	No	domain name resolution	Name server	53
ME, Probes	TCP	8071	XML-RPC	No	RPC server of raw traffic dumper	Probes	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	8888	XML-RPC	No	RPC config port for rtpanalyzer	Probes	Random
ME	UDP	1062	SNMP	No	binds counters	Not applicable	Not applicable
ME	TCP	3306	MYSQL	No	MySQL Server TCP connection connects vsi, acd, diamond, meco, ccalls, vsp, counters, regs	Not applicable	Not applicable
ME	TCP	4739	IPFIX	No	IPFIX communication with the SBC	SBC	Random
ME	TCP	4740	IPFIX	YES	IPFIX communication with the SBC	SBC	Random
ME	TCP	4741	IPFIX	No	IPFIX communication with the probe	probes	Random
ME	TCP	4742	IPFIX	YES	IPFIX communication with the probe	probes	Random
ME	TCP	5090	SIP	No	port to send SIP publish to the Vqcollector	Any	Random
ME	TCP	5555-5559	ZMQ-RPC	No	Counters manager publishes cnt changes to counters	Internal(vsi, meco, acd, diamond, apid)	Random
ME	TCP	6379-6389	REDIS	No	redis connects to vsi diamond and sau	Not applicable	Not applicable
ME	TCP	8077	XML-RPC	No	counter connects to vsp	Not applicable	Not applicable

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	8080	XML-RPC	No	vsi connects to vsp, vsictl.py	ME, Probe	Not applicable
ME	TCP	8081	HTTP	No	VSP connects nginx	Not applicable	Not applicable
AE	TCP	8095	HTTP	No	SAU REST interface, only bound on LO binds - sau connect - external	External	Not applicable
ME	TCP	8184	XML-RPC	No	apid XMLRPC listener connects to VSP	Internal(Apid)	Random
ME	TCP	8186	ZMQ-RPC	No	Counter manager publishes cnt changes to VSI binds - vsi connects - counter manager	Internal(VSI)	Random
ME	TCP	8188	ZMQ-RPC	No	Megaco probe ZMQ-PB-RPC port	Internal	Random
ME	TCP	8189	ZMQ-RPC	No	MGCP probe ZMQ-PB-RPC port	Internal	Random
ME	TCP	8190	ZMQ-RPC	No	ENUM probe ZMQ-PB-RPC port	Internal	Random
ME	TCP	8191	ZMQ-RPC	No	DIAMETER probe ZMQ-PB-RPC port	Internal	Random
Probe	TCP	8192	ZMQ-RPC	No	rat (RTP sniffer) ZMQ-PB-RPC port	Internal	Random
ME	TCP	8193	ZMQ-RPC	No	ccalls probe ZMQ-PB-RPC port	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	8194	ZMQ-RPC	No	apid probe ZMQ-PB-RPC port	Internal	Random
Probe	TCP	8195	ZMQ-RPC	No	rapid ZMQ-PB-RPC port	Internal	Random
ME	TC	10001	ZMQ-RPC	No	Megaco probe XMLRPC configuration bind - megaco_probe, connect - vsp	Internal	Random
ME	TCP	10002	XML-RPC	No	acd connects to vsp(ACD correlation XMLRPC configuration) binds - acd connects - vsp	Internal	Random
ME	TCP	10005	XML-RPC	No	MGCP probe XMLRPC configuration bind - mgcp_probe, connect - vsp	Internal	Random
ME	TCP	10009	XML-RPC	No	ENUM probe XMLRPC configuration binds - enum_probe connects - vsp	Internal	Random
ME	TCP	10013	XML-RPC	No	DIAMETER probe XMLRPC configuration bind - diameter_probe, connect - vsp	Internal	Random
ME	TCP	10017	ZMQ-DATPUB	No	vsi counter publish (ZMQ-JSON) endpoint	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	10019	XMLRPC	No	usd XMLRPC interface	Internal	Random
ME	TCP	10021	ZMQ-RPC	No	vsi alias update publish endpoint (ZMQ-ProtoBuf interface vsi-usd)	Internal	Random
ME	TCP	10023	XMLRPC	No	meco (Media Correlator) XMLRPC server port meco connects to vsp	Internal	Random
ME	TCP	10024	ZMQ-RPC	No	Counter manager publiches cnt changes to meco meco connects to counter manager	Internal	Random
ME	TCP	10025	ZMQ-DATPUB	No	meco connects to vsi meco (Media Correlator) ZMQ publisher (meco to VSI). This port is used by MECO to publish media leg reports (VQsummary data) to VSI.	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	10026	ZMQ-DATPUB	No	vsi connects to meco VSI ZMQ publisher for Media Leg Updates (VSI to meco). This port is used by VSI to send media related data about a call (by checking the SDP pairs) to MECO so that MECO can correlate it with RTP data.	Internal	Random
ME	TCP	10027	ZMQ-DATPUB	No	meco to counters_reader meco (Media Correlator) counter publish (ZMQ-JSON) endpoint port	Internal	Random
	TCP	10028	ZMQ-DATPUB	No	Diamond counter publish (ZMQ-JSON) endpoint port Diamond connects to counter_reader	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	10030	ZMQ-DATPUB	No	apid connects to vsi apid (ZMQ-JSON) endpoint port (subscribed by VSI for VQ data	Internal	Random
ME	TCP	10038	ZMQ-DATPUB	No	sdnp connects to vsi sdnp (ZMQ-JSON) endpoint port (subscribed by VSI for VQ data	Internal	Random
No NODE	TCP	10034	XMLRPC	No	diamond XMLRPC server port	Internal	Random
ME	TCP	10555	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd1 (counters values daemon of vsi cnts)	Internal	Random
ME	TCP	10556	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd2 (counters values daemon of meco cnts)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	10557	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd3 (counters values daemon of meco cnts)	Internal	Random
ME	TCP	10558	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd4 (counters values daemon of diamond cnts)	Internal	Random
ME	TCP	10559	XMLRPC	No	counters reader connects to counters manager Counters manager retrieves counter values from reader cvd5 (counters values daemon of apid cnts)	Internal	Random
ME	TCP	12000	ZMQ-DATPUB	Yes	vsi callstats target port (binds VSI connects fdpcallevents)	Fraud Monitor	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	12010	XMLRPC	No	export-metrics XMLRPC server (used by VSP for configuration injection)	Internal	Random
ME	TCP	18010	ZMQ-PKTPUB	No	apid SIP publisher apid (binds) connects to vsi	Internal	Random
probe	TCP	18015	ZMQ-PKTPUB	No	binds rat, connects rapid, ZMQ SIP publisher	Internal	Random
probe	TCP	18018	ZMQ-PKTPUB	No	binds rat, connects rapid, ZMQ Enum publisher (frames)	Internal	Random
probe	TCP	18019	ZMQ-PKTPUB	No	binds rat, connects rapid, ZMQ diameter publisher (frames)	Internal	Random
Probe	TCP	18027	ZMQ-DATPUB	No	rat daemon (RTP sniffer) RTP statistics publisher Publish statistics related to RTP and RTCP. Rat(bind) rapid(connect)	Internal	Random
ME	TCP	18028	ZMQ-DATPUB	No	megaco_probe(bind) acd (connect) Megaco Control to acd	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	18029	ZMQ-DATPUB	No	mgcp_probe(bind) acd (connect) Mgcp Control to acd	Internal	Random
ME	TCP	18030	ZMQ-DATPUB	No	Enum_probe(bind) acd (connect) Enum Control to acd	Internal	Random
ME	TCP	18031	ZMQ-DATPUB	No	diameter_probe(bind) acd (connect) Diameter(CX) Control to acd	Internal	Random
Probe	TCP	18032	ZMQ-PKTPUB	No	rat(bind) rapid(connect)rat daemon packet publisher. Publish recorded RTP/RTCP packets.	Internal	Random
Probe	TCP	18033	ZMQ-DATSUB	No	rat(bind) rapid(connect) rat daemon listen port for RecordRequest subscriber	Internal	Random
ME	TCP	19016	ZMQ-PKTPUB	No	megaco_probe(bind) acd (connect) MEGACO frames forwarded to acd	Internal	Random
ME	TCP	19017	ZMQ-PKTPUB	No	mgcp_probe(bind) acd (connect) MGCP frames forwarded to acd	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	19018	ZMQ-PKTPUB	No	enum_probe(bind) acd (connect) ENUM frames forwarded to acd	Internal	Random
ME	TCP	19019	ZMQ-PKTPUB	No	diameter_probe(bind) acd (connect) Diameter_cx frames forwarded to acd	Internal	Random
ME	TCP	10031	ZMQ-DATPUB	No	acd(bind) vsi (connect) acd to vsi protocol leg report	Internal	Random
ME	TCP	10032	ZMQ-DATPUB	No	vsi(bind) acd(connect) vsi to acd call leg updates	Internal	Random
ME	TCP	10035	ZMQ-DATPUB	No	acd(bind) counter(connect) acd counter publishing port, counters daemon connects to it	Internal	Random
ME	TCP	10036	ZMQ-DATPUB	No	apid(bind) counter(connect)apid counter publishing port	Internal	Random
ME	TCP	10037	ZMQ-DATPUB	No	apid(bind)meco(connect) apid (ZMQ-Protobuf) endpoint port (subscribed by MECO for VQ chunks)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	10033	ZMQ-RPC	No	acd(bind) counters manager(connect) counter manager publishes cnt changes to acd	Internal	Random
ME	TCP	18054	ZMQ-PUBSUB	No	Encapsulated frames as a result of a forward_cmd message.. Pint(bind) meco(connect)	Internal	Random
ME	TCP	18060	ZMQ-DATPUB	No	ZMQ vsi publisher (DB calls update data) (vsi publishes, ccalls subscribes)vsi(bind) ccalls(connect)	Internal	Random
ME	TCP	18061	ZMQ-DATPUB	No	ZMQ vsi publisher (DB registration event data (vsi publishes, ccalls subscribes)vsi(bind) ccalls(connect)	Internal	Random
ME	TCP	18062	ZMQ-DATPUB	No	ZMQ vsi publisher (DB subscription event data(vsi publishes, ccalls subscribes) vsi(bind) ccalls(connect)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	18115	ZMQ-PKTPUB	No	ZMQ SIP publisher apid(bind) vsi (connect)	Internal	Random
ME	TCP	18116	ZMQ-PKTPUB	No	ZMQ Megaco publisher (frames) apid(bind) megaco_probe (connect)	Internal	Random
ME	TCP	18117	ZMQ-PKTPUB	No	ZMQ mgcp publisher (frames) apid(bind) mgcp_probe (connect)	Internal	Random
ME	TCP	18118	ZMQ-PKTPUB	No	ZMQ enum publisher (frames) apid(bind) enum_probe (connect)	Internal	Random
ME	TCP	18119	ZMQ-PKTPUB	No	ZMQ diameter publisher (frames) apid(bind) diameter_probe (connect)	Internal	Random
ME	TCP	18127	ZMQ-DATPUB	No	rat daemon (RTP sniffer) RTP statistics publisher Publish statistics related to RTP and RTCP. Apid(bind) meco(connect)	Internal	Random

Node	Transport	Port	Protocol	Encrypted	Function	Remote Endpoint	Remote Port
ME	TCP	18132	ZMQ-PKTPUB	No	rat daemon packet publisher. Publish recorded RTP/RTCP packets. Apid(bind) meco(connect)	Internal	Random
ME	TCP	18133	ZMQ-DATSUB	No	rat daemon listen port for RecordRequest subscriber Apid(bind) meco(connect)	Internal	Random
ME	TCP	18150	ZMQ-DATPUB	No	Packet inspector info publisher. Apid(bind) pint(connect)	Internal	Random
ME	TCP	18151	ZMQ-DATPUB	No	Packet inspector search interface. Apid(bind) pint(connect)	Internal	Random
ME	TCP	18200	ZMQ-PKTPUB	No	apid Diameter publisher for DSC integration with CPM apid(bind) diameter(connect)	Internal	Random
ME, probe, AE	TCP	18300	HTTPS	Yes	Skype for Business SDN API updates subscriber port sdnp(bind) nginx(connect)	Internal	Random