

Oracle® Communications Session Monitor

Upgrade Guide



Release 6.1
G41896-01
December 2025

ORACLE®

Copyright © 2014, 2025, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About this Guide

Revision History

1 Upgrading Session Monitor

Supported Upgrade Paths	1
Pre-requisites	1
Configuring Proxies and Repos	1
Creating a Backup before Upgrading (Optional)	2
A Note if you Have Not Taken a Backup	2
Password Policy Changes	2
Upgrading Session Monitor from Release 5.1 or 5.2 or 6.0 to Release 6.1	3
Re-configuring Proxies	3
Downloading the Session Monitor Software	4
Upgrading the Session Monitor Software with Internet Connectivity	4
Enabling or Disabling SELinux After Upgrading	5
Upgrading Session Monitor without an Internet Connection	6
Prerequisites	6
Downloading Dependent RPMs on a Linux Machine with Internet Connectivity	7
Installing Any New Package on the Session Monitor Server	8
Enabling or Disabling SELinux After Upgrading	8

2 Upgrading DPDK

Uninstalling DPDK	1
Installing and Configuring DPDK with Internet for Intel	1
Installing and Configuring DPDK without Internet for Intel	2
Downloading, Installing, and Configuring DPDK for Mellanox NIC Cards	4
Installing DOCA OFED	4
Installing and Configuring DPDK	5
DPDK with Higher Throughput	6

3 Upgrading MySQL

About this Guide

This guide provides guidelines and recommendations for setting up Oracle Communications Session Monitor in a secure configuration. The Oracle Communications Session Monitor product family includes the following products:

- Operations Monitor
- Enterprise Operations Monitor
- Control Plane Monitor

Documentation Set

Table 1 Documentation Suite for Session Monitor Release 6.1

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.
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 Release 6.1, 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
December 2025	Initial Release. Includes documentation for new and enhanced features in the Oracle Communications Session MonitorRelease 6.1.

1

Upgrading Session Monitor

This document provides instructions for upgrading Oracle Communications Session Monitor from a previous version such as:

- Release 5.1 to Release 6.1
- Release 5.2 to Release 6.1
- Release 6.0 to Release 6.1

Supported Upgrade Paths

Session Monitor Release 5.1 is the minimum requirement for upgrading to Release 6.1. Verify that your current Session Monitor installation is listed as a valid upgrade path below. The possible upgrade paths to Release 6.1 are listed below.

Table 1-1 Supported Upgrade Paths

From	To	Mechanism	Backup and Restore
6.0	6.1	CLI upgrade	Optional
5.2	6.1	CLI upgrade	Optional
5.1	6.1	CLI upgrade	Optional

Note

It is recommended to have both Probe and Mediation Engine in the same version of Release 6.1.

Pre-requisites

Before beginning with the process of upgrading, ensure that the following pre-requisites are fulfilled.

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 proxy's address to the environment.

1. In **/etc/yum.conf**, add the following line:

```
proxy=<proxy_server>
```

2. Export the proxy's address.

```
export http_proxy=<proxy_server>
export https_proxy=<proxy_server>
```

Creating a Backup before Upgrading (Optional)

This procedure is optional but is recommended.

Session Monitor enables you to back up the Configuration, Database, Block Storage and essential Session Monitor files of the Session Monitor Servers by providing a Backup and Restore procedure.

For more information, see the Session Monitor Release 6.1 Backup and Restore Guide.

Note

Currently, there is no rollback option available from an upgrade.

A Note if you Have Not Taken a Backup

Create Historical System Diagnostics with the **Create savepoint** and **Include mysqldump** check boxes enabled from the PSA Page. This is mandatory.

Download a copy of the Diagnostics created and save it in a safe location. These diagnostics are required to debug any issues in the future.

For more information, see the System Diagnostics section in the Session Monitor Release 6.1 Installation Guide.

Note

Creating the Savepoint is applicable only for the Mediation Engine. Also, enabling the **Create savepoint** and **Include mysqldump** check boxes is mandatory for taking Diagnostics.

Password Policy Changes

From Session Monitor Release 6.1, changes in password policy have been introduced. Password Policy 1 and 2 present in the **Secure password policy** system setting are now considered insecure and are no longer available since Release 6.1. Only password policy 3 has been retained and this is the only and default option.

For existing users, if there are any users whose password is encrypted using password policy 1, then Session Monitor does not allow upgrade for such systems.

During the upgrade, a pre-test runs to check if any user has password encrypted using password policy 1 – the upgrade fails with the message:

```
Below users have an insecure password hash created using policy 1
Please change 'Secure password policy' to 3 in the 'System Settings' and change
the passwords accordingly...
```


If the above situation arises, then perform the following steps:

1. Set the Secure password policy to 3 in the **System Settings**.
2. Manually change the passwords of the users whose names appear in the message.
3. Try to upgrade again. This time it should be successful. Post a successful upgrade, **System Settings > Secure Password Policy** is set to 3.

For a fresh installation, the **Secure Password Policy** is set to 3 by default, and there is no option to change it.

Savepoint Restore on Session Monitor Release 6.1 will fail if any user has password encrypted using password policy 1. Perform the fix as given below:

1. Perform Step 1 and Step 2 given above.
2. Re-create the Savepoint.
3. Try to restore.

Upgrading Session Monitor from Release 5.1 or 5.2 or 6.0 to Release 6.1

Upgrade of Session Monitor from Releases 5.1, 5.2 or 6.0 to Release 6.1 is available only through a CLI upgrade.

1. For Mediation Engines, it is recommended to disconnect all probes.
2. Run the following command to stop Session Monitor service:

```
source /opt/oracle/ocsm/ocsm_env.sh  
pld-systemctl stop
```

3. Run the following command to stop the MySQL services:

```
systemctl stop mysqld
```

4. Upgrade to Oracle Linux 9.6 latest version.

Note

Refer to [Oracle Linux Upgrade Steps](#)

5. Run the following command to verify that Oracle Linux 9.6 has been installed:

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

You are required to re-configure the proxies. For more information, see [Re-configuring Proxies](#).

Re-configuring Proxies

You need to re-configure the proxies.

Configure the http proxy in the `/etc/yum.conf` file and also export the same to environment.

1. Add the following line in the `/etc/yum.conf`:

```
proxy=<proxy_server>
```

2. Export the proxy's address.

```
export http_proxy=<proxy_server>
export https_proxy=<proxy_server>
```

Downloading the Session Monitor Software

Perform the following tasks to download the Session Monitor Release 6.1 software:

1. Create a temporary directory (`temp_dir`) on the system that hosts the Session Monitor.
2. Download the Session Monitor installation software Zip file to the `temp_dir` folder from the My Oracle Support (MOS) website or the Oracle Software Delivery Website (OSDC).
3. Extract the Session Monitor installation software Zip file using `unzip`.

Upgrading the Session Monitor Software with Internet Connectivity

Upgrading the Session Monitor software

1. Install the Kernel version 5.15.0-302.167.6

- a. Enable the `ol9_UEKR7` repository:

```
dnf config-manager --set-enabled ol9_UEKR7
```

- b. Install the kernel:

```
dnf install -y kernel-uek-5.15.0-302.167.6.el9uek.x86_64
```

- c. Verify the grub configuration and check installed kernel is listed:

```
grubby --info=ALL | grep -E "^kernel|^index"
```

- d. Set the default kernel:

```
grubby --set-default=/boot/vmlinuz-5.15.0-302.167.6.el9uek.x86_64
```

- e. Reboot the system:

```
reboot
```

- f. Verify the kernel version after reboot:

```
uname -a
```

2. Once the VM or Server is up and running with 5.15 kernel, then uninstall 6.x kernel using the following commands:

```
rpm -qa | grep '^kernel-uek' | grep 6.12
dnf remove <6.12 kernel packages>
```

3. Ensure that the installation script has the executable permission. If not, then set it by executing below command.

```
chmod +x ./scripts/Upgrade_OCSM_Rel_6.1.sh
```

Note

Session Monitor Installation may take several minutes depending on the data size of MySQL.

4. Upgrade Session Monitor and its dependencies using this command.

```
./scripts/Upgrade_OCSM_Rel_6.1.sh ocsn-<rn>-RPM-GA.zip
```

where: <rn> is the current Session Monitor release number.

For example:

```
ocsm-6.1.0.0.0-RPM-GA.zip
```

Note

If any data loss occurs post upgrade, follow the Restore procedure provided in the Backup and Restore Guide.

Note

URLs of the Session Monitor Nodes have been updated since version Release 6.1 as below:

- https://<machine_ip>/me/
- https://<machine_ip>/mec/
- https://<machine_ip>/setup

Enabling or Disabling SELinux After Upgrading

After upgrading to Session Monitor Release 6.1, it is mandatory to enable or disable SELinux again as per your requirement.

SELinux policy modules have changed with Session Monitor Release 6.1, For more information, see the section Enabling SELinux in the Session Monitor Release 6.1 Installation Guide.

Enabling SELinux After the Upgrade

After the upgrade, it is mandatory to enable or disable SELinux again as per your requirement.

- To enable SELinux run the following commands:

1. Run these commands:

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

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

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

Disabling SELinux After the Upgrade

After the upgrade, it is mandatory to enable or disable SELinux again as per your requirement.

- To disable SELinux:
- Run the following commands:

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

Upgrading Session Monitor without an Internet Connection

Note

Offline upgrade for Oracle Linux from 8.x to 9.x is not supported; therefore, OCSM Offline upgrade functionality is also unavailable. Instead, users are advised to follow the backup and restore process as described in the Backup and Restore Guide.

Prerequisites

You can upgrade Session Monitor in an offline mode using any one of the methods listed here:

- Method 1: Session Monitor node acts as the repo server.
- Method 2: A separate node acts as the repo server.

Session Monitor upgrade requires a temporary Repo server to resolve the package dependencies. Going forward, this server will be referred to as the Repo server in this document.

The Repo server can be a part of the Session Monitor node itself (Method 1) OR it can be separate node (Method 2). If it is a separate node, the Session Monitor node must be able to reach the Repo server. In both methods, it is assumed that as the Session Monitor node does not have an internet connectivity, so the dependency RPM files and packages must be first downloaded on a machine which has the internet connectivity.

Note

This procedure was tested on:

- Oracle Linux 9.6
- MySQL 8.4.6
- MySQL Connector 8.4.0

The versions of Dependency RPMs used in this procedure are the latest available versions at the time of this release based on Oracle Linux 9.6 and MySQL 8.4.6 and the RPM file for Session Monitor Release 6.1.0.0.0. Use the latest version of dependency RPMs for all future patch releases based on the Oracle Linux, MySQL and Session Monitor RPM used.

Downloading Dependent RPMs on a Linux Machine with Internet Connectivity

Follow instructions in this section to download dependent RPMs on a Linux machine with internet connectivity. This Linux system should have 5 GB to 10 GB free disk space in the `/tmp` folder. Session Monitor.

1. Log in to the Linux machine as a root user OR root privileged user.
2. If the `/tmp/ocsm` folder already exists, take a backup of the `/tmp/ocsm` folder if required and delete the folder `/tmp/ocsm`.
3. Create a folder in `/tmp/ocsm`.

```
mkdir /tmp/ocsm
```

4. Copy the Session Monitor software Zip file, which is downloaded from My Oracle Support (MOS) or Oracle Software Delivery Cloud (OSDC) website, under the `/tmp/ocsm` folder on the Linux System.
5. Install the unzip package if not installed already.

```
yum install -y unzip
```

6. Change to folder `/tmp/ocsm`.

```
cd /tmp/ocsm
```

7. Unzip the software ZIP file which is copied here. For example:

```
unzip ocsn-6.1.0.0.0-GA.zip
```

8. Execute below steps to copy the Offline installation scripts to `/tmp/ocsm` folder.

```
cp -rf scripts/Offline_Installation/* /tmp/ocsm/
```

9. Set execute permission as:

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

10. Run the following command to download the script:

```
./Download_rpms.sh
```

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]"
```

Note

In the above command:

- PROTOCOL is HTTP or HTTPS
- HOST is the IP address or FQDN of the proxy server
- PORT is the port number for the proxy server

Installing Any New Package on the Session Monitor Server

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

To install any new package on the Session Monitor Server:

1. Download the required rpm and their dependencies 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 Session Monitor Server, execute the following command:

```
yum clean all
```

5. Install the package on the Session Monitor 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.

Enabling or Disabling SELinux After Upgrading

After upgrading to Session Monitor Release 6.1, it is mandatory to enable or disable SELinux again as per your requirement.

SELinux policy modules have changed with Session Monitor Release 6.1, For more information, see the section Enabling SELinux in the Session Monitor Release 6.1 Installation Guide.

Enabling SELinux After the Upgrade

After the upgrade, it is mandatory to enable or disable SELinux again as per your requirement.

- To enable SELinux run the following commands:

1. Run these commands:

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

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

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

Disabling SELinux After the Upgrade

After the upgrade, it is mandatory to enable or disable SELinux again as per your requirement.

- To disable SELinux:
 - Run the following commands:

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

2

Upgrading DPDK

DPDK upgrade is required. Session Monitor Release 6.1 and above supports DPDK version 24.11.2 only.

To update DPDK:

1. Follow the instructions in [Uninstalling DPDK](#).
2. Follow the instructions in [Installing and Configuring DPDK with Internet for Intel](#) or [Installing and Configuring DPDK without Internet for Intel](#) based on the set up below.
3. Reboot the machine that hosts the probe, or mediation engine and probe.

Uninstalling DPDK

This section describes the instructions for uninstalling DPDK.

To uninstall DPDK:

- Run the following commands:

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

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

Installing and Configuring DPDK with Internet for Intel

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-requisites:

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 tar
yum install -y git
yum install -y gcc-toolset-14.x86_64
git clone http://dpdk.org/git/dpdk-kmods (This command is to be executed
in root folder)
```

5. Edit /etc/default/grub and set "GRUB_ENABLE_BLSCFG" to False.
6. After making the changes in grub, run the command:

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

7. Execute this command in the root folder.

```
scl enable gcc-toolset-14 '/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.

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

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

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

Installing and Configuring DPDK without Internet for Intel

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 and install 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-5.15.0-302.167.6.el9uek.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. After downloading the RPM file, run this command:

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

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

7. Copy the downloaded `dpdk-kmods` folder into **root** of the system where DPDK needs to be installed.
8. Download the latest `.whl` files for the meson, ninja and pyelftools libraries from the URLs mentioned below:

Table 2-1 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

9. 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-14.x86_64
```

10. Edit `/etc/default/grub` and set "GRUB_ENABLE_BLSCFG" to False.

11. After making the changes in grub, run the command:

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

12. Clone the DPDK kernel modules repository from the official source using the command (Execute this command in root folder):

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

13. Execute this command in the root folder:

```
scl enable gcc-toolset-14 '/opt/oracle/ocsm/usr/share/pld/rat/  
configure_dpdk.py'
```

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

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

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

Downloading, Installing, and Configuring DPDK for Mellanox NIC Cards

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

Note

Starting with DPDK 24.11.2, support for Mellanox OFED has been terminated and has been migrated to DOCA OFED. Follow the instructions to install the DOCA OFED.

1. [Installing DOCA OFED](#)
2. [Installing and Configuring DPDK](#)

Installing DOCA OFED

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

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

Ensure that you have installed:

- Oracle Linux 9.6
- Session Monitor Release 6.1
- DPDK Version 24.11.2

1. Download the DOCA OFED based on OS distribution and architecture from the [NVIDIA DOCA 3.1.0 Downloads](#) page. Please follow the steps as mentioned below:

```
Select "Host Server" >> "DOCA-Host" >>
"Linux" >> "x86_64" >> "doca-ofed" >>
"OracleLinux" >> "9.6" >> Select on "rpm(local)"
```

2. Run the commands:
 - a. Run the following command to install the DOCA Host 3.1.0 package on the system:

```
sudo rpm -i doca-host-3.1.0-091000_25.07_ol96.x86_64.rpm
sudo dnf clean all
```

- b. Execute this command and verify if ol9_UEK7 repo is enabled or not.

```
sudo dnf repolist all | grep -i uek
```

- c. If the repo ol9_UEK7 is disabled, enable it using command:

```
sudo dnf config-manager --enable ol9_UEK7
```

3. Install the DOCA OFED package to enable the required network drivers and libraries. Use the command below:

```
sudo dnf -y install doca-ofed
```

Reboot once the installation is complete.

4. 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/python3.11` option.

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

5. 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 -y tar
yum install gcc-toolset-14.x86_64
```

6. Edit `/etc/default/grub` and set “GRUB_ENABLE_BLSCFG” to False. Once the changes are made in grub, run the command:

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

7. Run this command:

```
scl enable gcc-toolset-14 '/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`

DPDK with Higher Throughput

Starting with Session Monitor Release 5.1, 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.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`.

3

Upgrading MySQL

The MySQL upgrade occurs as a part of the Session Monitor Release 6.1 upgrade. For more information, see the section, upgrading Session Monitor.