Oracle® Communications Session Delivery Manager

Installation Guide

Release 8.0

September 2018

ORACLE

Oracle Communications Session Delivery Manager Installation Guide, Release 8.0

Contents

List of Figures

List of Tables

About This Guide

This document and other product-related documents are described in the Related Documentation table.

> **Note:**
>
> With the introduction of the product plugin service and changes in the SDM product, only the Oracle Communications Session Delivery Manager Documentation Library appears in this section of each SDM guide.

Related Documentation

Table 1 Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	Provides the following administration information: • Implement SDM on your network as a standalone server or high availability (HA) server. • Login to the SDM application, access GUI menus including help, customize the SDM application, and change your password. • Access the product plugin service through the GUI to manage product plugin tasks, including how product plugins are uploaded and installed. • Manage security, faults, and transport layer security certificates for east-west peer SDM server communication, and southbound communication with network function (NF) devices. • Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems. • Monitor SDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics. • Maintain SDM server operations, which includes database backup and database restoration and performing server cluster operations. • Use available SDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the SDM server.
Installation Guide	Provides the following installation information: • Do pre-installation tasks, which include reviewing system requirements, adjusting linux and firewall settings, completing SDM server settings and configuring your NNCentral account for security reasons. • Do the typical installation to perform the minimal configuration required to run the SDM server. • Do the custom installation to perform more advanced configurations including the mail server, cluster management, Route Manager, transport layer security (TLS), and Oracle database configuration.

Table 1 (Cont.) Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Release Notes	Contains information about the administration and software configuration of the SDM feature support new to this release.
Security Guide	Provides the following security guidelines: • Use guidelines to perform a secure installation of SDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines. • Review Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system. • Follow a checklist to securely deploy SDM on your network and maintain security updates.
REST API Guide	Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a network service orchestrator (NSO), to interact with SDM and its supported product plugins.
SOAP API Guide	The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programing model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the SDM server and data structures that are used as input and output parameters for these operations.

Revision History

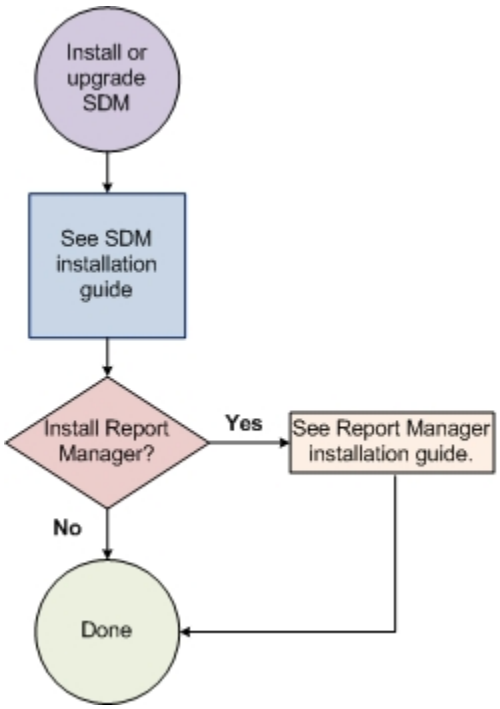
Date	Description
August 2017	Initial release
October 2017	Certain steps and examples were improved by making the SDM installation directory and software version number generic instead of specific in all examples.
November 2017	A caution note was added to the *Verify the Required SDM_localhost Entry is in the Hosts File* section.
May 2018	• In the *Configure Transport Layer Security Certificates* section of the *Custom Installation chapter*, a note was added that states that the importation or deletion of HTTPS certificates for the web service are not discussed, but it is discussed in the *Configure Web Server Security* section. • In the *Configure Web Server Security* section of the *Typical Installation* chapter, a note was added that states that this section does not discuss the importation or deletion of Transport Layer security certificates, but it is discussed in the *Configure Transport Layer Security Certificates* section.
September 2018	The *Check the File Descriptor Count on Your Linux System* section was added to the *Pre-Installation Tasks* chapter.

1
Pre-Installation Tasks

Read and understand the summary of pre-installation tasks that need to be done before installing Oracle Communications Session Delivery Manager. Each of these pre-installation tasks are described in more detail in subsequent sections.

1. If you have a software version of SDM that is installed on your system that is older than SDM, Release 7.5M3, you must upgrade to SDM, Release 7.5M3 before you can install SDM, Release 8.x.
2. Once the SDM system is installed and operational, use the instructions in the *Oracle Communications Session Delivery Manager Administration Guide* for more information regarding the installation of service provider and enterprise product plugins.
3. Read and understand this guide to install SDM for the first time or when you upgrade SDM from a previous version. You must do the SDM installation before you can install Oracle Communications Report Manager. Refer to the flow diagram below for more information:

Figure 1-1 Installing or upgrading SDM with Report Manager



4. Check to ensure your system meets the minimum requirements.
5. Shut down your SDM server and shut down all applicable server nodes (if you have SDM deployed as a server cluster).
6. Upgrade the version of Linux on your server(s) on which SDM is running, if the version of Linux is not supported with the release of SDM that you are installing.

7. Open the appropriate ports on the network and system firewall.
8. If your system does not rely on DNS, edit the /etc/hosts file to specify a host name for your system and verify that the required SDM_localhost entry is in the /etc/hosts file.
9. Disable the default httpd daemon.
10. Specify your system locale to the US English language UTF-8 character encoding method (LANG=en_US.UTF-8).
11. If any required Linux software libraries that are shared with SDM are missing, you must install them using the yum program.

> **Note:**
>
> Your system may already have these software libraries.

12. Setup the nncentral group and user account to administer SDM server operations on your Linux server.
13. Decide what type of installation for SDM that you want to do (Easy-Install, Headless, Typical, and Custom) based on the setup options that are available for each installation type.
14. Start the SDM installation.

Check System Requirements

Oracle has certified the following hardware ai

nd software server platforms as well as client requirements for use with Oracle Communications Session Delivery Manager.

> **Note:**
>
> Other hardware configurations might work with Oracle Communications Session Delivery Manager, but Oracle has verified the configurations listed here.

Oracle Communications Session Delivery Manager Server Requirements

- CPU: 4-core 2.1 GHz processor or better
- 16 GB RAM minimum, 24 GB RAM recommended
- 300 GB hard drive minimum

Supported Operating Systems

Oracle supports the following installations of Oracle Communications Session Delivery Manager:

- Oracle Linux 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2 64-bit.

> **Note:**
>
> OpenSSL 1.0.1e-fips or later must be installed on your linux server in order to use the HTTPS service on the Apache web server. Most Linux distributions include OpenSSL as part of the OS installation. You can check the version on your system by using the following command:
>
> ```
> openssl version
> OpenSSL 1.0.1e-fips 11 Jun 2017
> ```

Oracle supports the following installations of Oracle Communications Session Delivery Manager with Oracle Communications Report Manager:

- Oracle Communications Report Manager for Oracle Fusion Middleware 12c is supported on Oracle Linux (64-bit) 7.0, 7.1, 7.2, or 7.3
- Oracle Communications Report Manager for Oracle Fusion Middleware 11g is supported on Oracle Linux 6.5, 6.6, 6.7, 6.8 only.

Client Requirements

- Oracle recommends Internet Explorer versions 11.0 and later, Mozilla Firefox versions 43.3.1 and later, or Google Chrome version 56 and later.
- A Flash player compatible with your browser that is installed locally.
- If the server is not part of your DNS domain, the hosts file on each client must be edited to include the host name and IP address of the Oracle Communications Session Delivery Manager server.

Language Requirements

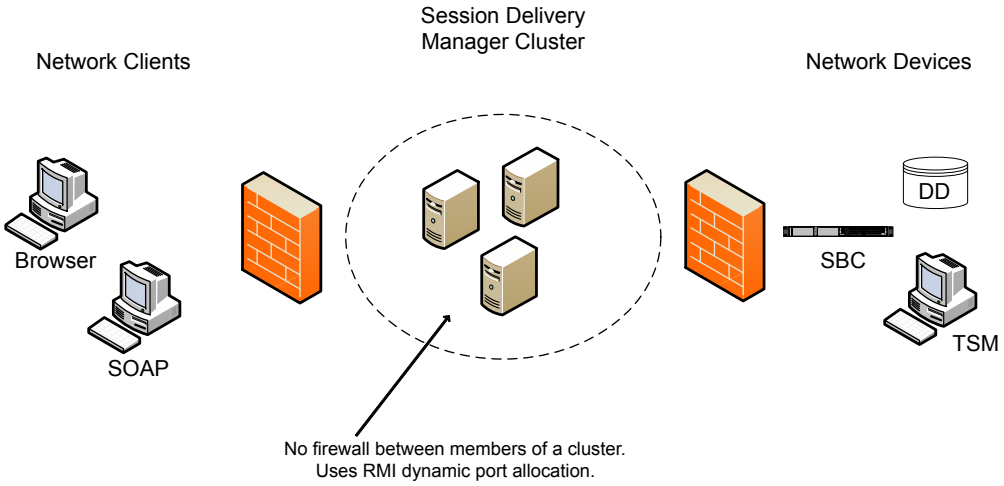
On the Linux server, ensure that the US English language UTF-8 character encoding method is specified.

Check Cluster Requirements

- All cluster nodes must reside at the same geographical location (be co-located).
- All cluster nodes must belong to the same IP network.
- No firewalls can exist between cluster nodes.
- Firewalls can exist between client browsers and the cluster nodes and product devices managed by a product plugin if their logical ports are specified when you install the cluster. Refer to the Check Firewall Settings section for more information.

Check Firewall Settings

When setting up Oracle Communications Session Delivery Manager (SDM) in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the SDM cluster, and a firewall between the SDM cluster and other devices.



Note:

You cannot have firewalls between the servers in a cluster.

If firewalls exist on either side of the SDM cluster, ensure the ports listed in the following table are open. If your operating system comes with a firewall, you need to apply the same criteria. You must switch off the firewall in your operating system or ensure these ports are available.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
Between SDM Cluster and Network Clients					
8443	TCP	HTTPS	N	Y	Apache port. HTTPS port for client/server communication.
8080	HTTP	HTTP	N	Y	HTTP port for client/server communication.
Between SDM Cluster and Network Devices					
161	UDP	SNMP	N	Y	SNMP traffic between the SDM server and the device.
162	UDP	SNMP	N	Y	SNMP trap reporting from the device to the SDM server.
22/21	SFTP/FTP				Used for file transfer (such as Route Manager and LRT updates).
8080	HTTP	AMI	N	Y	Used by SDM to communicate with 9200 devices via AMI.
5060	TCP		N	Y	Used for SDM Trunk Manager (SIPTX) to communicate with SP-SBC.
3001/ 3000		ACP/ACLI			Used by SDM to communicate with all versions of the device except for the Acme Packet 9200.
Between SDM Servers in the Cluster					
1098	TCP	RMI	N	Y	RMI Communication between host members in a cluster.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
1099	TCP	RMI Lookup	N	Y	RMI registry port. Used for the RMI communication between host members in a cluster.
5701	TCP	Hazelcast	N		Used by Hazelcast communication for distributed data structures, peer-to-peer collective data distribution.
5000/ 5801	TCP	Hazelcast	N	Y	Used by the Hazelcast management console port for the SDM distributed scheduler service.
54327	UDP	Hazelcast	N	Y	Used by Hazelcast for cluster member discovery.
8005	TCP	HTTP	N	Y	Tomcat shutdown port used by the shutdown script. Can be blocked on a firewall because it is local to the SDM server.
8009	TCP	Apache	N	Y	Tomcat port.
9000	TCP	Berkeley	N	Y	Berkeley database.
61616	TCP	Apache	N	Y	Message broker.
22	TCP	SFTP	N	Y	Used to transfer files between SDM servers.

Either port 8080 (HTTP) or port 8443 (HTTPS) must be open on the firewall, depending on which port you select between the network client and SDM server.

> **Note:**
>
> Ports are assigned dynamically through Remote Method Invocation (RMI) dynamic port allocation. If you are enabling and configuring iptables, all traffic must be allowed between servers in the cluster. Communication between clustered SDM servers must not be restricted.

Software Installation Prerequisites

Before you start the installation of Oracle Communications Session Delivery Manager you must check the following prerequisites.

Session Delivery Manager Installation

Ensure that you are currently running Oracle Communications Session Delivery Manager, Release 7.5M3 before you upgrade to Oracle Communications Session Delivery Manager, Release 8.0. If you are running any version of Oracle Communications Session Delivery Manager prior to Release 7.5M3, you cannot install Oracle Communications Session Delivery Manager, Release 8.0.

Check that Work Orders are in a Committed State

If you are upgrading from the previous version of Oracle Communications Session Delivery Manager, you must check the status of scheduled work orders before you upgrade to SDM Release 8.0.

All work orders must be in a **Committed** state before you upgrade to SDM, Release 8.0 because the migration of existing work orders on a server running SDM, Release 7.5m3 is not provided when you upgrade to SDM, Release 8.0. See your product plugin documentation for more information about placing your work orders into a **Committed** state.

Report Manager Installation

If you are installing the Oracle Communications Session Delivery Manager product software for the first time or upgrading from a previous version, complete the instructions in the *Oracle Communications Session Delivery Manager Installation Guide* before installing Oracle Communications Report Manager.

Upgrade to a Supported Version of Linux

Use this task if you have an unsupported version of Linux that needs to be upgraded to a supported version of Linux so you can install Oracle Communications Session Delivery Manager on your server.

Upgrade Linux on Your Server

Use this task if you need to upgrade the Linux server operating system on your server in order to upgrade Oracle Communications Session Delivery Manager.

> **Note:**
>
> Ensure that the server is shut down before you do this task. See the *Shut Down Your System* section for more information on shutting down the SDM server.

1. Login to the server as the nncentral user.
2. Change to the SDM software installation bin directory. For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Run the **backupdbcold.sh** script.

   > **Note:**
   >
   > The **backupdbcold.sh -- help** script provides all of the arguments that you can use.

   ```
   ./backupdbcold.sh
   ```

   - You can use the following arguments with this script:

- **-d** —Use this argument to select a local directory that you want to store backup archives. For example:

  ```
  ./backupdbcold.sh -d/<sdm-install-directory>/AcmePacket/<Directory>/
  NNC<version>_ColdBackup_yyyy_mm_dd_<number>_all.tar
  ```

- **-a**, **--all** — Use this argument to run all backups and store them as a single archive.

  ```
  ./backupdbcold.sh --all
  ```

- **-c --core** — Use this argument to backup the core application database and store it as an individual archive.

  ```
  ./backupdbcold.sh --core
  ```

- **-r --report** — Use this argument to backup the reporting Oracle database and repository and store as an individual archive.

  ```
  ./backupdbcold.sh --report
  ```

- **-o --ocsdmdw** — Use this argument to backup the (Oracle Communications Session Delivery Manager Data Warehouse (OCSDMDW) database and store as an individual archive.

  ```
  ./backupdbcold.sh --ocsdmdw
  ```

- **-ep**, **--excludePlugins** —Use this argument to exclude archived plugin zip files from the resulting backup file. By default, the resulting backup file contains all product plugin installation zip files which were previously uploaded to SDM. You can override this behavior by entering this command.

  ```
  ./backupdbcold.sh --excludePlugins
  ```

After the script runs, the output displays a section called **Backup Results**. The output shows if the core SDM application database and reporting databases are successfully backed up to the default **DatabaseBackup** directory. The following example shows the directory on which the application database file was backed up:

```
/<sdm-install-directory>/AcmePacket/DatabaseBackup/
NNC<version>_ColdBackup_yyyy_mm_dd_<number>_all.tar
```

> **Note:**
>
> If you do not have reporting configured on the SDM server, the output shows that the reporting databases failed to be backed up.

4. Upgrade the server to a supported version of Linux. See *Check System Requirements* for more information.
5. Repeat the steps above if you need to upgrade another Linux server on which Oracle Communications Session Delivery Manager needs to run.

Check the File Descriptor Count on Your Linux System

The Oracle Communications Session Delivery Manager server requires that the Linux system, on which it is installed and runs, have 20,000 file descriptors.

1. Login to the server as the nncentral user.
2. Use the `ulimit -n` command to view the number of file descriptors configured for your Linux system.

   ```
   ulimit -n
   ```

3. If the output displays a value of 20000 or greater, you are finished with this task. If the output value is less than 20000, continue to the next step.
4. Navigate to the SDM installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

5. Run the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

   > **Note:**
   >
   > However, You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.

   ```
   ./shutdownnnc.sh
   Shutdown back-end server
   Do you wish to shut down the entire cluster (Yes/No)? Yes
   ```

6. Login to the server as the root user.
7. Open the limits.conf file in the `/etc/security/` directory to check if there is any line in the file with `soft nofile` or `hard nofile` entries. For example:

   ```
   /etc/security/limits.conf
   #<domain>      <type>          <item>              <value>

   *               soft            nofile               20000
   *               hard            nofile               20000
   ```

8. If there are no values after the `nofile` entries or these entries are less than 20000, enter each entry as shown above.
9. Exit the shell.
10. Login to the server as the nncentral user.
11. Use the `ulimit -n` command again to view the number of file descriptors that you configured (the command should now return a value of 20000).
12. If you have a cluster setup, repeat the previous steps for each cluster member.

Verify the Required SDM_localhost Entry is in the Hosts File

You must verify that the required `SDM_localhost` entry is in the `/etc/hosts` file that is used for internal server communication within a cluster, or for any SDM server(s) in your environment that do not rely on a domain name server (DNS).

> **Note:**
>
> The IP address that is used for the `SDM_localhost` entry on each SDM cluster member must be registered on the network Domain Name Server (DNS). If this entry is absent on the DNS server, DNS lookup timeouts occur, which can cause database problems.

1. Login to the server as the root user.
2. Enter the **ifconfig** command to view the Ethernet 0 (`eth0`) IP address on the SDM server.

   ```
   [my_linux_system]$ ifconfig

   eth0      Link encap:Ethernet  HWaddr 00:21:F6:69:00:33
             inet addr:10.138.222.189  Bcast:10.138.223.255  Mask:255.255.252.0
             inet6 addr: fe80::221:f6ff:fe69:33/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:31991154 errors:0 dropped:0 overruns:0 frame:0
             TX packets:10798060 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:2842355697 (2.6 GiB)  TX bytes:26025276531 (24.2 GiB)
             Interrupt:163
   ```

3. View the `/etc/hosts` file to verify that there is a `SDM_localhost` entry and that the IP address of this entry matches the `eth0` interface.

   The following example has the correct `eth0` interface (shown in the previous example) and `SDM_localhost` entry:

   ```
   [my_linux_system]$ Vi /etc/hosts
   10.138.222.189 acme189 SDM_localhost
   ```

4. If the `/etc/hosts` file does not include the `eth0` IP address and `SDM_localhost` entries, enter them in the `/etc/hosts` file using the following format:

   > **Note:**
   >
   > The order in which this entry appears in the hosts file does not matter.

   For example:

   ```
   <eth0 IP address> <optional hostname(s)> SDM_localhost
   ```

> **Note:**
>
> SDM_localhost does not support IPv6 link-local addresses.

If you fail to add the `SDM_localhost` entry in the hosts file, the following message appears during the SDM setup installation process:

```
Setup encountered an error and cannot continue!
INVALID_SERVICE_CONFIGURATION: /etc/hosts file is not configured correctly.
There should be one entry for SDM_localhost. Please refer to the
installation documents for proper syntax.
```

5. Restart the network service to initialize the changes that you made to the `hosts` file.

   ```
   $ service network restart
   ```

Disable the Default HTTP Daemon

If your Oracle Communications Session Delivery Manager server is running a default HTTP daemon (HTTPD) process, disable that process from restarting.

1. Login to the server as the root user.
2. To discover if the HTTPD is installed or running:

   ```
   service httpd status
   ```

   The following message appears if the HTTPD is not installed. Continue to the next sections.

   ```
   httpd: unrecognized service
   ```

   The following message appears if the HTTPD is installed but not running. Continue to the next sections.

   ```
   httpd is stopped
   ```

   A message similar to the following appears if the HTTPD is installed and running:

   ```
   httpd (pid 5644) is running...
   ```

3. If the HTTPD is running, stop the HTTPD:

   ```
   service httpd stop
   ```

4. Disable the HTTPD from restarting when the system reboots:

   ```
   chkconfig httpd off
   ```

5. Verify that the HTTPD is not running:

   ```
   service httpd status
   ```

> **Note:**
>
> If your are using Oracle Linux 7 or later, use the following command:
>
> ```
> systemctl status httpd
> ```

Specify the System Locale

You must specify the system location to LANG=en_US.UTF-8 (United States English language) in order for Oracle Communications Session Delivery Manager to install properly.

1. Login to the server as the root user.
2. Ensure that the US English language UTF-8 character encoding method (LANG=en_US.UTF-8) parameter is specified in the i18n (Internationalization) file in the /etc/sysconfig/i18n directory. This file specifies the current language settings.

Resolve Any Oracle Linux 6 Installation Dependencies

Resolve any Oracle Linux 6.5, 6.6, 6.7, 6.8 software library dependencies before you install SDM so that the SDM installation process runs properly:

Table 1-1 Oracle Linux 6 software library packages shared with Oracle Communications Session Delivery Manager

Name	Description
apr	The Apache Portable Runtime (APR) supporting library is for the Apache web server that provides a set of application programming interfaces (APIs) that map to the underlying operating system (OS). The APR provides emulation where the OS does not support a particular function to make a program portable across different platforms.
apr-util	The APR Utility Library (APR-Util) provides a predictable and consistent interface for underlying client library interfaces. This API assures predictable if not identical behavior regardless of which libraries are available on a given platform.
compat-expat1	Expat is a stream-oriented parser for XML documents. You register handlers with the parser before starting the parse and these handlers are called when the parser discovers the associated structures in the document being parsed. A start tag is an example of the kind of structures for which you may register handlers.
libxslt	The package contains extensible style sheet language transformations (XSLT) libraries. These are useful for extending libxml2 libraries that are used to manipulate XML files to support XSLT files.
libaprutil	The APR database binding library for the Apache web server.
libGL	OpenGL-based programs must link with the libGL library that implements the GLX interface as well as the main OpenGL API entry points.
libX11	The X.Org stack, which provides an open source implementation of the X Window System for the C language X interface. See the X.Org Foundation for more information.
libXxf86vm	X11 XFree86 video mode extension library provides an interface to the XFree86-VidModeExtension extension, which allows client applications to get and set video mode timings in extensive detail. It is used by the xvidtune program in particular.
alsa-lib	Advanced Linux Sound Architecture (ALSA) library package used by programs (including ALSA Utilities) requiring access to the ALSA sound interface.

If you are missing any shared software libraries in your Oracle Linux environment, run the "yum" program. Yum is the primary tool for getting, installing, deleting, querying, and

managing Oracle Linux software packages from official software repositories, as well as other third-party repositories.

1. Login to your Oracle Linux system on which SDM is to be installed as the **root** user.
2. Install the Oracle Linux software on your linux system using the "yum" program. For example:

```
yum install -y apr
```

Resolve Any Oracle Linux 7 Installation Dependencies

Resolve any of the following Oracle Linux 7.0 or later software library dependencies before you install SDM so that the SDM installation process runs properly:

Table 1-2 Linux software library packages shared with SDM

Name	Description
apr	The Apache Portable Runtime (APR) supporting library is for the Apache web server that provides a set of application programming interfaces (APIs) that map to the underlying operating system (OS). The APR provides emulation where the OS does not support a particular function to make a program portable across different platforms.
apr-util	The APR Utility Library (APR-Util) provides a predictable and consistent interface for underlying client library interfaces. This API assures predictable if not identical behavior regardless of which libraries are available on a given platform.
libxslt	The package contains extensible style sheet language transformations (XSLT) libraries. These are useful for extending libxml2 libraries that are used to manipulate XML files to support XSLT files.
libaprutil	The APR database binding library for the Apache web server.
libGL	OpenGL-based programs must link with the libGL library that implements the GLX interface as well as the main OpenGL API entry points.
libX11	The X.Org stack, which provides an open source implementation of the X Window System for the C language X interface. See the X.Org Foundation for more information.
libXxf86vm	X11 XFree86 video mode extension library provides an interface to the XFree86-VidModeExtension extension, which allows client applications to get and set video mode timings in extensive detail. It is used by the xvidtune program in particular.
alsa-lib	Advanced Linux Sound Architecture (ALSA) library package used by programs (including ALSA Utilities) requiring access to the ALSA sound interface.

If you are missing any shared software libraries in your Oracle Linux environment, run the "yum" program. Yum is the primary tool for getting, installing, deleting, querying, and managing Oracle Linux software packages from official software repositories, as well as other third-party repositories.

1. Login to your Oracle Linux system on which SDM is to be installed as the **root** user.
2. Install the Oracle Linux software on your linux system using the "yum" program. For example:

```
yum install -y apr-util
```

Configure the NNCentral Account

For security reasons, you must create an NNCentral user account named nncentral and an NNCentral group named nncentral on the server to administer Oracle Communications Session Delivery Manager related server operations. You also must specify limited sudo privileges for the nncentral user and nncentral group. After the Oracle Communications Session Delivery Manager installation, all the installed files are owned by the nncentral account. The main Oracle Communications Session Delivery Manager process has to run as a sudo user in order to have access to port 162.

Add the NNCentral Group and NNCentral User Account

The nncentral group and user account must be added to administer Oracle Communications Session Delivery Manager server operations on your Linux server.

1. Login to the server as the root user.
2. Add the nncentral group

   ```
   groupadd nncentral
   ```

3. Add the nncentral user account.

   ```
   useradd -m -g nncentral -d /home/nncentral -s /bin/bash nncentral
   ```

4. Set the password for the nncentral user.

   ```
   passwd nncentral
   ```

5. If you are prompted to enter a new password, reenter the password that you entered in step 4.

   The following message displays:

   ```
   passwd: all authentication tokens updated successfully.
   ```

Specify NNCentral User Privileges

You must specify limited privileges for an NNCentral user on the Linux server, so this user can administer Oracle Communications Session Delivery Manager operations on the server.

You must use `visudo` to make edits to the sudoer configuration file.

> **Note:**
>
> This file can only be edited using Linux visual text editor (vi editor) commands.

1. Login to the server as the root user.
2. Execute visudo.

   ```
   # visudo
   ```

3. Press **i** to enter insert mode and begin adding text.
4. Add the following line to specify NNCentral user privileges in the sudoer configuration to give the NNCentral user the limited authority to run Oracle Communications Session Delivery Manager:

> **Note:**
>
> The placeholder <my-sdm-install-directory> is the name of the directory where you installed SDM and the command line as shown below is not valid without modification. Also, the entire entry must be entered on the same line. Take notice also that the example below may wrap as it is shown, depending on how you are viewing this document (HTML or PDF).

```
nncentral ALL=/<my-sdm-install-directory>/AcmePacket/NNC*/jre/bin/java * -
Dlog4j.configuration*=* -cp *
com.acmepacket.ems.server.services.snmp.TrapRelay.TrapRelay *
```

5. Press Esc to return to command mode.
6. Press **:wq** to save your changes and exit visudo.

> **Note:**
>
> If you want to quit without saving your changes, press **:q!**.

7. Ensure that the sudoer configuration for the nncentral user is specified.

```
grep nncentral /etc/sudoers
```

2
Typical Installation

The Typical installation performs the minimal configuration required to run the Oracle Communications Session Delivery Manager server.

The following tasks are accomplished in the Typical installation:

1. The setup program loads and installs the appropriate product plugins (if you are upgrading SDM from a previous version).

> **Note:**
>
> If you are installing SDM for the first time, the appropriate product plugins must be installed after the SDM server installation. See the *Manage Product Plugins* chapter in the *Oracle Communications Session Delivery Manager Administration Guide* for more information.

2. You can configure passwords for the default user accounts.
3. You can configure the global identifier
4. You can either configure HTTP or HTTPS (recommended) on the Apache web server.
5. You can configure the SNMP Trap Relay port for Fault Manager.

> **Note:**
>
> Verify you have the correct sudo password before continuing.

Install a New Session Delivery Manager Standalone Server

Ensure that you do the following tasks before you start a new SDM standalone server installation:

1. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.0 for more information about the names and descriptions of the software files that you need to do this upgrade.
2. Download the SDM application image file to a directory on the server on which you are installing SDM.
3. Unzip the application image file. See the *Unzip the Tar File to Create the Installation Directory* section for more information.
4. Start the installation. See the *Start the New Standalone Installation* section for more information.

Unzip the Tar File to Create the Session Delivery Manager Installation Directory

Use this task to unzip the tar file containing the Oracle Communications Session Delivery Manager software application image and create the SDM installation directory called AcmePacket.

1. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.x for more information about the names and descriptions of the software files that you need.
2. Download the appropriate tar.gz (application image) file from the Oracle customer portal to a directory on the server where you want to install SDM.
3. Login to your server as the root user.
4. Navigate to the directory where you want to install SDM on the server.

   ```
   cd /<directory>
   ```
5. Extract the tar.gz file.

   For example:

   ```
   tar -xzvf NNC<version>OracleLinux65_64bit.tar.gz
   ```

   or

   ```
   tar -xzvf NNC<version>OracleLinux70_64bit.tar.gz
   ```

   The SDM (AcmePacket) software installation directory is created. For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

Start the Standalone Installation

1. Login to the server as the root user.
2. Navigate to the Oracle Communications Session Delivery Manager installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```
3. Run the setup application with the setup.sh script.

   ```
   ./setup.sh
   ```

> **Note:**
>
> A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.

> **WARNING:**
>
> This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.

4. continue.
5. Complete the SDM installation and press Enter to continue to the setup, where you can select your SDM installation type. Depending on the SDM installation type you choose, refer to the Typical Installation, Custom Installation, Easy Installation, or Headless Installation chapter for more information.

Install a New Session Delivery Manager Cluster

You can install a high-availability (HA) cluster of SDM servers to ensure reliable, continuous data and operations by masking both planned and unplanned downtime and preventing single points of failure without compromising availability.

An SDM cluster is comprised of multiple server nodes (members), each of which can be a candidate node for your file systems, databases or applications. Each cluster node monitors the health of other cluster nodes. If a node fails, another node in the cluster takes over services for the failed node. For example, when an interruption or failure occurs in a critical application on a node, a high-availability cluster combats this disruption by switching application operations to another node within the cluster to quickly and seamlessly prevent a complete system failure.

Ensure that you do the following tasks before you start a new SDM cluster installation:

1. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.0 for more information about the names and descriptions of the software files that you need to do this upgrade.
2. Download the SDM application image file to a directory to each server (cluster) node on which you are installing SDM.
3. Unzip the application image file on each server node in the cluster. See the *Unzip the Tar File to Create the Installation Directory* section for more information.
4. Start the installation and complete the Typical Installation on each server node in the cluster. See the *Start the New Cluster Installation* section for more information.
5. After the Typical Installation on each server node in the cluster is complete, see the Configure a New Cluster in the Custom Installation chapter for more information on associating the cluster nodes that you installed with each other so that they can function together as a cluster.

Unzip the Tar File to Create the Session Delivery Manager Installation Directory

Use this task to unzip the tar file containing the Oracle Communications Session Delivery Manager software application image and create the SDM installation directory called AcmePacket.

1. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.x for more information about the names and descriptions of the software files that you need.

2. Download the appropriate tar.gz (application image) file from the Oracle customer portal to a directory on the server where you want to install SDM.
3. Login to your server as the root user.
4. Navigate to the directory where you want to install SDM on the server.

   ```
   cd /<directory>
   ```
5. Extract the tar.gz file.

   For example:

   ```
   tar -xzvf NNC<version>OracleLinux65_64bit.tar.gz
   ```

   or

   ```
   tar -xzvf NNC<version>OracleLinux70_64bit.tar.gz
   ```

   The SDM (AcmePacket) software installation directory is created. For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

Start the Cluster Installation

You can install a high-availability (HA) cluster of SDM servers to ensure reliable, continuous data and operations by masking both planned and unplanned downtime and preventing single points of failure without compromising availability.

1. Login to your server as root user.
2. Navigate to the Oracle Communications Session Delivery Manager installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```
3. Run the setup.sh script.

   ```
   ./setup.sh
   ```

   Note:

   A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.

   WARNING:

   This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.
4. Complete the SDM installation and press Enter to continue to the setup, where you can select your SDM installation type. Depending on the SDM installation type you choose, refer to the Typical Installation, Custom Installation, Easy Installation, or Headless Installation chapter for more information.
5. Repeat the previous steps on each server node in the cluster.

6. After the each cluster node is complete, refer to the Configure the Installed Session Delivery Manager Cluster chapter for more information on associating the cluster nodes that you installed with each other so that they can function together as a cluster.

Configure a New Cluster

When configuring the Oracle Communications Session Delivery Manager cluster, add all other nodes each time you run setup.sh. For example, if you are setting up a cluster with nodes A, B, and C. When running setup.sh on node A, add nodes B and C; when running setup.sh on node B, add nodes A and C; and when running setup.sh on node C, add nodes A and B.

> **Note:**
>
> When configuring or modifying the master cluster server, all cluster replica nodes must be shut down.

1. Login to the server as the root user.
2. Navigate to the SDM installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Run the setup.sh script.

   ```
   ./setup.sh
   ```

   > **Note:**
   >
   > A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.

   > **WARNING:**
   >
   > This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.

4. Select option 2, **Custom**. Press Enter to continue.

   ```
   [ ]  1 - Typical : Runs through most common set up options. (Recommended)
   [Default]
   [X]  2 - Custom : Allows manual customization. (Advanced users)
   [ ]  3 - Quit : Finish and quit setup.
   ```

5. From the **Customize Configuration** menu (after you have started the custom installation), Select option 6, **Cluster management**. Press Enter to continue.
6. When you are prompted, enter **Yes** to continue.
7. Select option 1, **Configure and manage members in cluster**. Press Enter to continue.
8. When you are prompted, enter **Yes** to continue.

See additional sections in this chapter to perform other management operations on the cluster.

Add New Nodes to a Cluster

1. Select option 1, **Add a new member**. Press Enter to continue.
2. When you are prompted, enter the IP address of the node you are adding to the cluster. For example

   ```
   Provide the IP address of the Host requiring membership to cluster.
   Member IP address [ ]
   ```

   > **Note:**
   >
   > Do not enter the domain name server (DNS) name or the fully qualified domain name (FQDN) for the node.

3. Repeat steps to add additional nodes to the cluster.
4. When done adding nodes, select option 3, **Apply new cluster configuration**. Press Enter to continue.
5. Select option 3, **Quit out of cluster configuration**. Press Enter to continue.
6. If this system is not part of the cluster, select option 2, **No**. Otherwise, select option 1, **Yes**. Press Enter to continue.
7. If you selected **Yes**, enter the nncentral user name and nncentral password which other nodes of the cluster can use to SFTP files from this system. See the Configure the NNCentral Account section if you need to configure an nncentral account.

   > **Note:**
   >
   > The master server node in the SDM cluster must be started and fully operational before you can start the replica nodes.

Upgrade a Session Delivery Manager Standalone Server

> **Note:**
>
> Ensure that you are currently running SDM, Release 7.5M3. If you are running any version of SDM prior to Release 7.5M3, you cannot install SDM Release 8.0.

Use the following summary of tasks to upgrade your SDM standalone server:

1. Shut down your standalone SDM server. See the *Shutdown the System* section for more information.
2. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.0 for more

information about the names and descriptions of the software files that you need to do this upgrade.

3. Download the SDM application image file to the same base directory in which the Release 7.5M3 software was initially installed.
4. Unzip the application image file. See the *Unzip the Tar File to Create the Installation Directory* section for more information.
5. If you are upgrading Report Manager, the Oracle Database and Oracle BI Publisher must be running before you upgrade SDM so that Report Manager database data is migrated.
6. Start the installation.

Shut Down the Session Delivery Manager Server

You can shut down the existing Oracle Communications Session Delivery Manager software version running on your system to install a new version of the software, restore a database or apply a software patch. If you are upgrading an SDM cluster, use these steps to shut down each server node in the cluster.

1. Login to your server as the nncentral user.
2. Navigate to the SDM installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Run the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

   > **Note:**
   >
   > However, You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.

   ```
   ./shutdownnnc.sh
   Shutdown back-end server
   Do you wish to shut down the entire cluster (Yes/No)? Yes
   ```

Unzip the Tar File to Create the Session Delivery Manager Installation Directory

Use this task to unzip the tar file containing the Oracle Communications Session Delivery Manager software application image and create the SDM installation directory called AcmePacket.

1. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.x for more information about the names and descriptions of the software files that you need.
2. Download the appropriate tar.gz (application image) file from the Oracle customer portal to a directory on the server where you want to install SDM.
3. Login to your server as the root user.

4. Navigate to the directory where you want to install SDM on the server.

   ```
   cd /<directory>
   ```

5. Extract the tar.gz file.

   For example:

   ```
   tar -xzvf NNC<version>OracleLinux65_64bit.tar.gz
   ```

   or

   ```
   tar -xzvf NNC<version>OracleLinux70_64bit.tar.gz
   ```

   The SDM (AcmePacket) software installation directory is created. For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

Start the Session Delivery Manager Standalone Upgrade

> **Note:**
>
> The previous release of Oracle Communications Session Delivery Manager must manage at least one device to be upgraded successfully.

1. Login to your server as the root user.
2. Navigate to the SDM installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Run the setup application with the setup.sh script. The setup application determines that a migration of the application data needs to occur from the current release and that specific plugin(s) need to be installed based on the product devices (SBCs, E-SBCs, or both) SDM managed in the previous release.

   ```
   ./setup.sh
   ```

   > **Note:**
   >
   > A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.

   > **WARNING:**
   >
   > This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.

4. The data migration tool automatically detects the previous release. When you are prompted, select that you have a standalone system and use the following section to complete your upgrade.

Migrate Application Data on a Standalone System

Migrate the application data on the master node (member) of the cluster system.

1. Enter 1 to proceed with database migration.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by <enter>.
Note that database migration MUST be performed before setup can continue.
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

2. Enter Yes to migrate data from the previous Oracle Communications Session Delivery Manager installation.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No?  Yes
```

   Pressing a key anytime during the process aborts the current migration. You cannot be able to launch the target version of Oracle Communications Session Delivery Manager until setup is re-run and database migration is performed.

3. When you are prompted, specify the directory path on your server where you downloaded the requested product plugin(s). Once the directory path(s) to the product plugin(s) are provided, the migration process continues migrating SDM 7.5M3 application data to SDM 8.0.

4. Press Enter to continue the Typical Installation.

Upgrade a Session Delivery Manager Cluster

> **Note:**
>
> Ensure that you are currently running SDM, Release 7.5M3. If you are running any version of SDM prior to Release 7.5M3, you cannot install SDM Release 8.0.

Use following summary of tasks to upgrade your SDM server cluster:

1. Shut down all SDM server nodes. See the *Shutdown the System* section for more information.

2. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.0 for more information about the names and descriptions of the software files that you need to do this upgrade.

3. Download the SDM application image file to each SDM server cluster node in the same base directory in which the Release 7.5M3 software was initially installed.

4. Unzip the application image file on each SDM server cluster node. See the *Unzip the Tar File to Create the Installation Directory* section for more information.
5. If you are upgrading Report Manager, the Oracle Database and Oracle BI Publisher must be running before you upgrade SDM so that Report Manager database data is migrated.
6. Start the installation on the master cluster node and migrate the application data from the previous release to this master cluster node.
7. Continue the Typical Installation on the master node.
8. Migrate the application data from the previous release to each cluster replica node.
9. With the introduction of SDM, Release 8.0, you must select one server to start in the cluster only (which in this case is the master node). Once this server is started and operational, you can start the other server(s) in the cluster.

Shut Down the Session Delivery Manager Server

You can shut down the existing Oracle Communications Session Delivery Manager software version running on your system to install a new version of the software, restore a database or apply a software patch. If you are upgrading an SDM cluster, use these steps to shut down each server node in the cluster.

1. Login to your server as the nncentral user.
2. Navigate to the SDM installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Run the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

   > **Note:**
   >
   > However, You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.

   ```
   ./shutdownnnc.sh
   Shutdown back-end server
   Do you wish to shut down the entire cluster (Yes/No)? Yes
   ```

Unzip the Tar File to Create the Session Delivery Manager Installation Directory

Use this task to unzip the tar file containing the Oracle Communications Session Delivery Manager software application image and create the SDM installation directory called AcmePacket.

1. See the *Session Delivery Manager Software Distribution Media* section in the Oracle Communications Session Delivery Manager Release Notes, Release 8.x for more information about the names and descriptions of the software files that you need.

2. Download the appropriate tar.gz (application image) file from the Oracle customer portal to a directory on the server where you want to install SDM.
3. Login to your server as the root user.
4. Navigate to the directory where you want to install SDM on the server.

   ```
   cd /<directory>
   ```
5. Extract the tar.gz file.

   For example:

   ```
   tar -xzvf NNC<version>OracleLinux65_64bit.tar.gz
   ```

   or

   ```
   tar -xzvf NNC<version>OracleLinux70_64bit.tar.gz
   ```

   The SDM (AcmePacket) software installation directory is created. For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

Start the Session Delivery Manager Cluster Upgrade

> **Note:**
>
> The previous release of Oracle Communications Session Delivery Manager must manage at least one device to be upgraded successfully.

1. Login to the master cluster server node as the root user.
2. Navigate to the SDM installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```
3. Run the setup application with the setup.sh script. The setup.sh application determines that a migration of the application data needs to occur from the current version to 8.x. If you are migrating from SDM Release 7.5M3, specific plugin(s) may need to be installed based on the product devices (SBCs, E-SBCs, or both).

   ```
   ./setup.sh
   ```

   > **Note:**
   >
   > A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.

   > **WARNING:**
   >
   > This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.

4. The data migration tool automatically detects the previous release. When you are prompted, select that you have a clustered system and use the following section to complete your upgrade.

Migrate Application Data on the Master Cluster Node

Transfer the application data on the master node (member) of the cluster system.

1. Enter 1 to transfer application data from the previous Oracle Communications Session Delivery Manager installation.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by <enter>.
Note that database migration MUST be performed before setup can continue.
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

2. When prompted, enter Yes to transfer application data from the previous Oracle Communications Session Delivery Manager installation.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No?  Yes
```

3. When you are prompted, specify the directory path on your server where you downloaded the requested product plugin(s). Once the directory path(s) to the product plugin(s) are provided, the migration process continues migrating SDM 7.5M3 application data to SDM 8.0. During this process, the setup application asks you if you want to transfer a backup of the migrated database (DB) to other members of the cluster. If you answer yes, a backup is done and transferred to the targeted members of the server cluster.

4. Enter 1 to copy the transferred database to other cluster nodes.

```
Your existing setup is configured for a clustered environment.  Setup on all
other nodes in your cluster will require the migrated database archive just
created.  Setup can now attempt to copy this archive via SFTP to other
cluster
nodes.
Note that if you skip this step, you must manually copy the migrated database
archive to all other nodes in the cluster, as this archive will be required
during setup on the other cluster nodes
[X]  1 - Copy the migrated database archive to other cluster nodes
[Default]
[ ]  2 - Do not copy the migrated database archive
Please select an option [1] 1
```

5. When prompted, enter Yes to continue.

6. Enter the username, password, and folder path for the SFTP credentials for each cluster node when prompted.

```
Provide SFTP credentials for cluster node 2.2.2.2:
username:  [] myuser
password:  [] xxxxx
remote folder path:  [        ] /home/myuser
remote folder path:  [/home/myuser]
```

For example, a successful application data transfer shows information similar to the following:

```
cluster node: 2.2.2.2
destination file: /home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz
result:  SUCCEEDED
cluster node: 3.3.3.3
destination file: /home/otheruser/ColdBackup_2012_02_13_112911_db.tar.gz
result:  SUCCEEDED
Press <enter> to continue
Database migration is now complete.
Press <enter> to continue with setup
```

7. Press Enter and continue to the Typical Installation.
8. Once you have completed the Typical Installation on the master node, go to the Migrate Application Data on Each Cluster Replica Node section to complete the cluster upgrade on the replica nodes in the cluster.

Migrate Application Data on Each Cluster Replica Node

Transfer the application data to each replica node (member) of the cluster system.

Pre-requisites: Ensure that you have shut down the server, downloaded and unzipped the application image file, and started the setup application on the replica node before starting this task.

1. Enter 1 to continue importing the database backup.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by <enter>.
Note that database migration MUST be performed before setup can continue.
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

2. Enter Yes to continue.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
```

3. Enter 1 to continue.

```
Your existing setup is configured for a clustered environment.  For your
existing environment, setup must be run on cluster node 1.1.1.1 prior
to running setup on any other cluster node (including this one).  When setup
is run on cluster node 1.1.1.1, a migrated master database archive
file will be produced.
If you have already run setup on 1.1.1.1 and either allowed setup to
automatically copy the database archive file to this node, or have copied
this
file manually, please select option [1] below.  Otherwise, please select
option [2] below to cancel setup.  Then run setup on 1.1.1.1 before
running setup again on this node.
[X]  1 - Specify location of migrated master database archive file
[Default]
```

```
[ ]  2 - Cancel and exit setup
Please select an option [1] 1
```

4. Enter Yes to continue.

```
[X]  1 - Proceed with database migration   [Default]
[ ]  2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
```

5. Enter the full path to the database backup and enter yes to continue the import process.

```
Enter migrated master database archive file path:
[        ] /home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz
[/home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz]
backing up existing database....done
restoring the migrated master database...done
Restore migrated master database archive succeeded
Press <enter> to continue with setup
```

6. Press Enter to continue the Typical Installation and later the Custom Installation of Oracle Communications Session Delivery Manager (depending on your installation requirements of Oracle Communications Session Delivery Manager). These installation(s) must be completed to use the current Oracle Communications Session Delivery Manager software version on this replica node system.
7. Repeat the previous steps if you need to transfer application data on another replica node (member) of the cluster system.
8. Press Enter to continue the Typical Installation.

Transfer the Migrated Application Database Backup to the Replica Node Manually

Use this task if you opted not to copy the migrated database archive when you migrated application data on the master cluster node when upgrading SDM from a previous release.

1. Log into the replica node, shut it down and do a backup of the application database (also known as a cold backup). See the *Backup Databases on a Shutdown Server* section in the *Session Delivery Manager Server Database Maintenance* chapter of the *Oracle Communications Session Delivery Manager Administration Guide* for more information.
2. Migrate the application data on this replica node from the backed up application database. See the Migrate Application Data on Each Cluster Replica Node section in this chapter for more information.
3. Repeat the previous steps for any remaining cluster node.

Start the Typical Installation

1. Select option 1, **Typical**. Press Enter to continue.

```
[X] 1 - Typical : Runs through most common set up options. (Recommended)
[Default]
[ ] 2 - Custom : Allows manual customization.
[ ] 3 - Quit : Finish and quit setup.
```

Configure User Account Passwords

You need to configure passwords for the admin and LIadmin user groups before starting the Oracle Communications Session Delivery Manager application. Identical credentials must be configured during installation on all nodes of a clustered deployment.

1. Select option 1, **Enter Passwords for default user accounts that will be created**. Press Enter to continue.

```
[X]  1 - Enter Passwords for default user accounts that will be created
[Default]
[ ]  2 - Global identifier configuration
[ ]  3 - Web Server configuration
[ ]  4 - Fault Management configuration
[ ]  5 - Quit setup
```

2. Enter the admin password and confirm by re-entering it.
3. Enter the LIadmin password and confirm by re-entering it.

Specify the Global ID for Northbound Trap Receivers

The **OC SDM global identifier configuration** installation option must be configured on an Oracle Communications Session Delivery Manager server to create a unique global identifier (ID). When a device that is managed by Oracle Communications Session Delivery Manager forwards SNMP trap fault notifications, the global ID that you configure is used in this notification. When an administrator receives the SNMP trap fault notification on their northbound system, the originating device can be determined by viewing the global ID contained in the SNMP trap fault notification.

> **Note:**
>
> The global identifier must be the same for all nodes in a clustered system.

1. Select option 2, **OC SDM global identifier configuration**. Press Enter to continue.

```
[ ]  1 - Enter Passwords for default user accounts that will be created
[Default]
[X]  2 - Global identifier configuration
[ ]  3 - Web Server configuration
[ ]  4 - Fault Management configuration
[ ]  5 - Quit setup
```

2. Enter a global unique identifier for the system and press Enter. For example:

```
Enter global identifier: [ ] OCSDM
```

Configure Web Server Security

This task is used to configure the server to run in either HTTPS or HTTP mode, configure Apache web server parameters, and optionally configure the size of files being uploaded to the

web server for the secure functioning of the web server and Oracle Communications Session Delivery Manager.

> **Note:**
>
> This section does not discuss the importation or deletion of Transport Layer security certificates for east-west peer SDM server communication, and for southbound communication with network function (NF) devices. These actions are handled in the Custom Installation when using the SDM setup installation program. Refer to the Configure Transport Layer Security Certificates section for more information.

1. Select option 3, **Web Server configuration**. Press the Enter key to continue.
2. Option 1 (**HTTP/HTTPS configuration**) is selected by default to configure the your web server parameters. Press Enter to continue.

```
[X]  1 - HTTP/HTTPS configuration - Setup HTTP or HTTPS configuration
[Default]
[ ]  2 - Security configuration - Options below can be used to modify the
Web server security configurations of OCSDM
```

   a. We highly recommend that you keep HTTPS mode (default) as the system running mode for your system to create secure web connections. If you need HTTP (unsecured) select option 2. Press Enter to continue.

   > **Note:**
   >
   > OpenSSL 1.0.1e-fips or later must be installed on your linux server in order to use the HTTPS service on the Apache web server to support the options of running HTTPS with Transport Layer Security (TLS) 1.0, 1.1, and 1.2.

```
[X]  1 - HTTPS mode [Default]
[ ]  2 - HTTP mode
```

   b. Accept the default nncentral user as the Apache user.

   > **Note:**
   >
   > You cannot use the value **root** for the Apache user.

```
Apache User [nncentral]
```

   c. Accept the default nncentral group as the Apache group.

   > **Note:**
   >
   > You cannot use the value **root** for either the Apache group name.

```
Apache Group [nncentral]
```

d. Enter an Apache port number or accept the default port of 8443 (secure HTTPS).

> **Note:**
>
> Port 8080 is the port number for unsecured HTTP.

```
Apache Port Number (1024-65535) [8443]
```

e. Enter the DNS name of the server.

```
Server name [] myserver1
```

> **Note:**
>
> The specified DNS server name must match the common name (CN) of the certificate.

f. (For HTTPS configuration only) If your certificate is signed by a certificate authority, select option 2, **No**, when prompted about creating a self-signed certificate. Press Enter to continue. If your certificate is not signed, continue to sub-step **g**.

i. Enter the absolute path to the private key file.

```
Private key file []
```

ii. Enter the absolute path to the certificate file.

```
Certificate file []
```

iii. If there are intermediate certificates, select option 1. Press Enter to continue. Then enter the absolute path to the certificate chain file. Otherwise, select the default option 2.

```
Are there intermediate certificates?
[ ]  1 - Yes
[X]  2 - No   [Default]
```

g. If you want to create a self signed certificate, select option 1, **Yes**. Press Enter to continue.

h. Accent nncentral as the certificate alias name.

```
Certificate alias name [nncentral]
```

i. Specify a truststore password that provides write protection to the truststore where X.509 certificates are kept. X.509 certificates are used in many internet protocols, including TLS/SSL, which is the basis for HTTPS.

```
Truststore password []
```

The upper-level the security configuration is complete and the main web server menu returns. If you do not need to adjust the default maximum file size for files that are uploaded to the web server, your web server configuration is complete.

3. (Optional) Select option 2, **Security configuration** to update the Apache HTTP Daemon (HTTPD) server configuration files, if you need to change the default value set by Oracle Communications Session Delivery Manager for files that can be uploaded to the web server. Press the Enter key to continue.

```
[ ]  1 - HTTP/HTTPS configuration - Setup HTTP or HTTPS configuration
[Default]
[X]  2 - Security configuration - Options below can be used to modify the
Web server security configurations of OCSDM
```

a. Select option 1, `Modify web server file directive size limit [Default]`.

```
[X]  1 – Modify web server file directive size limit [Default]
[ ]  2 - Enable TLS versions 1.1 and 1.2 (HTTPS)
[ ]  3 – Cancel out and do not apply changes
```

b. Press Enter to continue.

```
[X]  1 – Modify web server file directive size limit [Default]
[ ]  2 - Enable TLS versions 1.1 and 1.2 (HTTPS)
[ ]  3 – Cancel out and do not apply changes
```

c. You are next prompted to enter the upload file size limit in gigabytes (GB). The default size limit is 2 gigabytes.

```
Web server File Size Limit in GB (2-100) [2]
```

If the entered value exceeds the file-size limit, an error message displays and prompts you to re-enter the value.

4. (Optional) By default, Transport Layer Security (TLS) 1.0 is used for HTTPS. Select option 2, **Security configuration** if you want to enable TLS versions 1.1 and 1.2 to be used for HTTPS instead.

```
[ ]  1 - HTTP/HTTPS configuration - Setup HTTP or HTTPS configuration
[Default]
[X]  2 - Security configuration - Options below can be used to modify the
Web server security configurations of OCSDM
```

a. Select option 2, `Enable TLS versions 1.1 and 1.2 (HTTPS)`.

```
[ ]  1 – Modify web server file directive size limit [Default]
[X]  2 - Enable TLS versions 1.1 and 1.2 (HTTPS)
[ ]  3 – Cancel out and do not apply changes
```

b. Press Enter to continue.

```
[ ]  1 – Modify web server file directive size limit [Default]
[X]  2 - Enable TLS versions 1.1 and 1.2 (HTTPS)
[ ]  3 – Cancel out and do not apply changes
```

Configure Fault Management

1. Select option 4, **Fault Management configuration**. Press Enter to continue.

```
[ ]  1 - Enter Passwords for default user accounts that will be created
[Default]
[ ]  2 - OC SDM global identifier configuration
[ ]  3 - HTTP/HTTPS configuration
[X]  4 - Fault Management configuration
[ ]  5 - Quit setup
```

2. Select option 1, **Configure SNMP trap settings**. Press Enter to continue.

```
[X]  1 - Configure SNMP trap settings   [Default]
[ ]  2 - Quit out of fault management configuration
```

3. Either enter the port number that your server will listen on for SNMP traps or press Enter to accept the default port of 162.

> **Note:**
>
> You cannot use a port number reserved for Oracle Communications Session Delivery Manager components.

```
Enter the port number that Trap Relay should listen on:  (1-65535) [162]
```

4. If prompted (you entered a port below 1024), enter the sudo password. Then re-enter the sudo password to confirm.

> **Note:**
>
> The sudo password is the NNCentral password to provide root permissions for listening for SNMP traps on ports lesser than port 1024.

5. Select option 5, **Quit setup**. Press Enter to continue.

Next Step
Start the Oracle Communications Session Delivery Manager server.

Start the Server after a Standalone Installation

1. Once the installation completes, switch to the nncentral user from the root user. For example:

   ```
   [root@myserver bin]# su nncentral
   ```

2. Navigate to the Oracle Communications Session Delivery Manager installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Start SDM with the startnnc.sh script.

   ```
   ./startnnc.sh
   ```

   After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up. If you are upgrading from 7.5M3, the plugin service management system automatically uploads the plugins from the path you identified earlier, and installs them. The console displays the number of services started. For example:

   ```
   Starting Back-End server now
   27 of 27 services have started...
   Starting Apache servers...

   Servers and services started successfully. Web client access ready.
   ```

4. Once the system is started, you can begin using SDM by entering the server host name or IP address, and port number in your web browser navigation bar.

   For example:

   ```
   https://example.com:8443
   ```

5. In the login page, enter the administrator login name and password that you configured in the Configure User Account Passwords section.

Next Steps

- Check SDM server processes.

Start the Server after a Cluster Installation

Use this task if you are starting the SDM server after the cluster installation.

> **Note:**
>
> Ensure that the application data migration from SDM 7.5M3 to SDM 8.x has successfully completed before starting the cluster.

1. Once the installation completes, switch to the nncentral user from the root user on any cluster node. For example:

   ```
   [root@myserver bin]# su nncentral
   ```

2. Navigate to the Oracle Communications Session Delivery Manager installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Start SDM with the startnnc.sh script.

   ```
   ./startnnc.sh
   ```

   After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up. If you are upgrading from 7.5M3, the plugin service management system automatically uploads the plugins from the path you identified earlier, and installs them. The console displays the number of services started. For example:

   ```
   Starting Back-End server now
   27 of 27 services have started...
   Starting Apache servers...

   Servers and services started successfully. Web client access ready.
   ```

4. Once the system is started, you can begin using SDM by entering the server host name or IP address, and port number in your web browser navigation bar.

   For example:

   ```
   https://example.com:8443
   ```

5. Once this server has started on this node and it is operational, you can start the other server node(s).

6. Enter the administrator login name and password that you configured in the Configure User Account Passwords section.

Next Steps

- Check SDM server processes.

Check Server Processes

After the startnnc.sh script has completed, you can verify that Oracle Communications Session Delivery Manager is up and running by entering the report process status command on the system. Depending on your hardware specifications it may take a few minutes for Oracle Communications Session Delivery Manager to start.

1. Execute the report process status command on the server.

   ```
   ps -eaf | grep Acme
   ```

   When Oracle Communications Session Delivery Manager is successfully running, you should see:

   - Several httpd processes
   - Three or more Java processes

2. If the above processes are running and you still cannot connect to your server, check the firewall settings of your server and network. See Firewall Settings in chapter 1.

3
Custom Installation

The custom installation options are for more advanced users. The following custom options are displayed :

- Mail server configuration
- Cluster management—See the Configure the New Cluster section in the *Typical Installation* chapter and the *Session Delivery Manager Server Cluster Maintenance* chapter in the *Oracle Communications Session Delivery Manager Administration Guide* for more information.
- Route Manager configuration
- Transport layer security (TLS) configuration
- Oracle Database configuration

> **Note:**
>
> The first four steps of the custom installation are identical to the steps of the typical installation.

Start the Custom Installation

1. Login to the server as the root user.
2. Navigate to the Oracle Communications Session Delivery Manager installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Run the setup application with the setup.sh script.

   ```
   ./setup.sh
   ```

> **Note:**
>
> A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.

> **WARNING:**
>
> This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.

4. Select option 2, **Custom**. Press Enter to continue.

```
[ ] 1 - Typical        : Runs through most common set up options.
(Recommended) [Default]
[X] 2 - Custom         : Allows manual customization.              (Advanced
users)
[ ] 3 - Easy-Install   : Prompts user for minimal setup option values.
[ ] 4 - Quit           : Finish and quit setup.
```

5. Enter Yes to continue.

   The following main custom installation options appear:

```
[X]  1 - Enter Passwords for default user accounts that will be created
[Default]
[ ]  2 - Global identifier
configuration
[ ]  3 - Web Server
configuration
[ ]  4 - Fault Management
configuration
[ ]  5 - Mail Server
configuration
[ ]  6 - Cluster
management
[ ]  7 - Route Manager Central
configuration
[ ]  8 - SAML Single sign on
configuration
[ ]  9 - SBI TLS
configuration
[ ]  10 - Oracle DB OCSDMDW configuration. Please drop this DB, if it
already exists.
[ ]  11 - Quit setup
```

> **Note:**
>
> Option 8, SAML Single sign on configuration for importing self-signed certificates into the Route Manager certificates file (cacerts), is not supported in this release.

Configure the Mail Server

> **Note:**
>
> If you want Session Delivery Manager products to send out emails, you can setup the mail server credentials to enable the sending of emails to a targeted Microsoft Exchange and Gmail server.

1. Select option 5, **Mail Server configuration**. Press Enter to continue.

```
[X] 5 - Mail Server configuration
```

2. Select option 1, **Configure mail server**. Press Enter to continue.

```
[X]  1 - Configure mail server   [Default]
```

3. Select option 1, **Configure mail server host**. Press Enter to continue.

```
[X]  1 - Configure mail server host
```

4. Enter the DNS name of your mail server.

```
Provide the DNS name.
Host name [] mail.example.com
```

5. Select option 1, **Mail server secure protocol**. Press Enter to continue.

```
[X]  1 - Mail server secure protocol
```

6. Select your mail server's secure protocol.

   Valid secure protocols are:

   - starttls
   - ssl

> **Note:**
>
> Customers may select none, but Oracle recommends all customers select starttls or ssl.

7. Select option 1, **Mail server port**. Press Enter to continue.

```
[X]  1 - Mail server port
```

8. Choose a port number or press Enter to select the default port 465.
9. Select option 1, **Configure mail from**. Press Enter to continue.

```
[X]  1 - Configure mail from
```

10. Enter the address you want used for the From address.

    For example, if sending to Microsoft Exchange account, mailadmin@acmepacket.com. If sending to a Gmail account, mailadmin@gmail.com.

```
Provide the mail from.
Mail from [ ] mailadmin@example.com
```

11. Select option 1, **Configure mail user**. Press Enter to continue.
12. Enter the mail user id.

```
Provide the mail user id.
Mail user [] user@example.com
```

13. Select option 1, **Configure mail logon required**. Press Enter to continue.
14. Select either true or false.

```
Mail logon required true/false [false]
```

    a. If you set the mail logon required to true, select option 1, **Configure mail logon user password**. Press Enter to continue.

```
[X]  1 - Configure mail logon user password
```

    b. Enter the mail logon user password.

```
Mail logon user password []
```

15. Select option 1, **Extra mail properties**. Press Enter to continue.

```
[X]  1 - Extra mail server properties   [Default]
```

16. Enter the extra mail server properties you want to configure.

    The format for entering multiple mail server properties is:

    ```
    property1:value1;property2:value2;property3:value3
    ```

17. Select option 2, **Apply new mail server configuration**. Press Enter to continue.
18. Select option 2, **Quit out of mail server configuration**. Press Enter to continue.

Configure Route Management Central

1. Select option 7, **Route Manager Central configuration**. Press Enter to continue.
2. Set the maximum number of route set backups.

    ```
    Please enter the maximum number of route set backups per route set/backup
    type combination
    # of backups (1-500) [10]
    ```

Configure Transport Layer Security Certificates

The transport layer security (TLS) feature provides a single secure sockets layer (SSL) keystore of entity or trusted certificates that provide support for all applications, product plugins, and their respective network functions that run on Oracle Communications Session Delivery Manager.

> **Note:**
>
> This section does not discuss the importation or deletion of HTTPS certificates for the web service. Refer to the Configure Web Server Security section for more information.

Configure Entity Certificates

1. Select option 9, **SBI TLS configuration**. Press Enter to continue.
2. Select option 1, **Entity Certificate**. Press Enter to continue.
3. Select option 1, **Create Entity Certificate**. Press Enter to continue.
4. Enter the certificate details.
    - Common name
    - Organization unit
    - Organization
    - City or locality
    - State or province
    - Country code
    - Key size
    - The number of days during which this certificate is valid

    After creating an Entity Certificate, new options appear.
5. Select the action you wish to perform.

- View Entity Certificates
- Export Entity Certificate
- Generate Certificate Signing Request (CSR)
- Import Signed Entity Certificate
- Delete Entity Certificates
- Return to Main Menu

6. If you select the option to export the certificate, import a certificate, or generate a CSR, provide the absolute path to the file.
7. When finished configuring the entity certificate, select option 6, **Quit and back to Main Menu**. Press Enter to continue.

Configure Trusted Certificates

1. Select option 9, **SBI TLS configuration**. Press Enter to continue.
2. Select option 2, **Trusted Certificate**. Press Enter to continue.
3. Select option 1, **Import Trusted Certificate**. Press Enter to continue.
4. Enter the alias name for the certificate.
5. Enter the full path to the certificate

   For example:

   ```
   Enter full path of the certificate to be imported: [ ] /etc/ssl/certs/
   server.crt
   ```

6. Select the action you wish to perform.
   - Import Trusted Certificate
   - List all Certificates
   - View Certificate detail
   - Delete Trusted Certificate
   - Return to Main Menu
7. If you select the option to view or delete a certificate, provide the alias of the certificate.
8. When finished configuring trusted certificates, selection option 5, **Quit and back to Main Menu**. Press Enter to continue.

About Creating a Report Manager Database Instance on the External Oracle Database

If you are using Oracle Communications Report Manager with Oracle Communications Session Delivery Manager, option 10 (Oracle DB OCSDMDW configuration) in the Custom Installation is used to specify the Oracle home path (ORACLE_HOME) and the credentials of the Oracle database user instance (OCSREMDW).

For more information about creating the OCSDMDW database instance, see the *Create a Report Manager Database Instance* chapter in the *Oracle Communication Report Manager Installation Guide*.

Exit the Custom Installation

1. Select option 11, **Quit setup**. Press Enter to continue.

Start the Server after a Standalone Installation

1. Once the installation completes, switch to the nncentral user from the root user. For example:

   ```
   [root@myserver bin]# su nncentral
   ```

2. Navigate to the Oracle Communications Session Delivery Manager installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Start SDM with the startnnc.sh script.

   ```
   ./startnnc.sh
   ```

   After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up. If you are upgrading from 7.5M3, the plugin service management system automatically uploads the plugins from the path you identified earlier, and installs them. The console displays the number of services started. For example:

   ```
   Starting Back-End server now
   27 of 27 services have started...
   Starting Apache servers...

   Servers and services started successfully. Web client access ready.
   ```

4. Once the system is started, you can begin using SDM by entering the server host name or IP address, and port number in your web browser navigation bar.

   For example:

   ```
   https://example.com:8443
   ```

5. In the login page, enter the administrator login name and password that you configured in the Configure User Account Passwords section.

Next Steps

- Check SDM server processes.

Start the Server after a Cluster Installation

Use this task if you are starting the SDM server after the cluster installation.

> **Note:**
>
> Ensure that the application data migration from SDM 7.5M3 to SDM 8.x has successfully completed before starting the cluster.

1. Once the installation completes, switch to the nncentral user from the root user on any cluster node. For example:

   ```
   [root@myserver bin]# su nncentral
   ```

2. Navigate to the Oracle Communications Session Delivery Manager installation bin directory.

   For example:

   ```
   cd /<sdm-install-directory>/AcmePacket/NNC<version>/bin
   ```

3. Start SDM with the startnnc.sh script.

   ```
   ./startnnc.sh
   ```

   After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up. If you are upgrading from 7.5M3, the plugin service management system automatically uploads the plugins from the path you identified earlier, and installs them. The console displays the number of services started. For example:

   ```
   Starting Back-End server now
   27 of 27 services have started...
   Starting Apache servers...

   Servers and services started successfully. Web client access ready.
   ```

4. Once the system is started, you can begin using SDM by entering the server host name or IP address, and port number in your web browser navigation bar.

   For example:

   ```
   https://example.com:8443
   ```

5. Once this server has started on this node and it is operational, you can start the other server node(s).

6. Enter the administrator login name and password that you configured in the Configure User Account Passwords section.

Next Steps

- Check SDM server processes.

Check Server Processes

After the startnnc.sh script has completed, you can verify that Oracle Communications Session Delivery Manager is up and running by entering the report process status command on the system. Depending on your hardware specifications it may take a few minutes for Oracle Communications Session Delivery Manager to start.

1. Execute the report process status command on the server.

   ```
   ps -eaf | grep Acme
   ```

   When Oracle Communications Session Delivery Manager is successfully running, you should see:

   - Several httpd processes
   - Three or more Java processes

2. If the above processes are running and you still cannot connect to your server, check the firewall settings of your server and network. See Firewall Settings in chapter 1.