

# **Oracle® Communications Session Delivery Manager**

Installation Guide

Release 7.4

*Formerly Net-Net Central*

June 2015

**ORACLE®**

## Notices

Copyright ©2015, 2012, Oracle and/or its affiliates. All rights reserved.

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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

## **1 Installation Prerequisites..... 7**

Overview.....	7
Hardware Support.....	7
SBC Support.....	8
Installation Prerequisites.....	8
System Requirements.....	8
Information You Need.....	9
Components Required.....	9
Firewall Settings.....	9
Oracle Linux VM.....	11
Deploying the OVM Template.....	12
Creating a Guest VM.....	13
Adding VNICs to the VM.....	14
Launching and Accessing the VM.....	14
Configuring the VM with Sysprep.....	15
Before a New Installation.....	20
Configuring Linux.....	20
User and Group Accounts.....	21
Installing Oracle Communications Session Delivery Manager.....	22
Installing Oracle Communications Session Delivery Manager.....	22
Running Setup.....	22
Typical Setup.....	24
Custom Installation.....	29
Accessing Custom Options.....	29
Mail Server.....	30
Cluster Management.....	33
Manage Cluster Members.....	34
Route Management Central.....	37
Installing Other Licensed Applications.....	39
Exiting Setup.....	40
Starting the NNC Server.....	40
Checking Running Processes.....	40
Shutting down the Server.....	41
Standalone System.....	41
Cluster System for NNC 7.0.....	41
Cluster System for NNC 7.1+.....	42
Configuring the Acme Packet SBC for Session Delivery Manager Interaction.....	42
Configuring the SNMP Interface.....	42
Starting the Oracle Communications Session Delivery Manager Client and Connecting to the Server.....	44
Verifying the Client System Settings.....	44
Starting the Oracle Communications Session Delivery Manager Client.....	45

## **2**

## **Migrating Data to the Oracle Communications Session Delivery Manager**

.....	<b>47</b>
Upgrading to Oracle Communications Session Delivery Manager 7.4.....	47
Requirements.....	47
Before You Migrate Data.....	47

Migrate Data from Older Versions of Net-Net Central.....	49
Upgrade SDM Across Platforms.....	51
Requirements.....	51
Before You Start.....	52
Upgrade the Server Platform.....	52
Migrate Data Across Platforms.....	52
Upgrade to SDM 7.4.....	53
Cluster Setup and Migration.....	53
EMS 6.x to Oracle Communications Session Delivery Manager 7.3.....	53
Migration Process.....	54
Requirements.....	54
Before You Migrate Data.....	54
Migrating Data from EMS 6.x to Oracle Communications Session Delivery Manager 7.3.....	55
Net-Net EMS 6.X to Oracle Communications Session Delivery Manager 7.3 Database Migration Information	56
.....	56
Running Database Migration Again.....	56
Data Migration Logging.....	57
Error Logging.....	58
Mapping Device Groups to User Groups.....	58
Migrating Route Manager Data.....	59
Migration Process.....	59
Requirements.....	59
Before You Migrate Data.....	59
Migrating from Route Manager 1.x.....	60

### 3

## Installing Oracle Communications Session Delivery Manager Patches.....63

Shutting Down Oracle Communications Session Delivery Manager Servers.....	64
Running the Patch Management Tool in a Cluster.....	64
Identifying the Master Node Patch Version in a Cluster.....	64
Installing Oracle Communications Session Delivery Manager Patches.....	64
Listing Imported Patches.....	65
Importing Patches.....	65
Applying Patches.....	66
Removing All Applied Patches.....	66
Re-establishing User-Configured Setup Configurations.....	67

## 4 Troubleshooting.....69

Missing Libraries.....	69
------------------------	----

---

## About this guide

The Oracle Communications Session Delivery Manager Installation Guide explains how to install the Session Delivery Management Suite, which provides advanced management applications and services.

### SDM File and Directory Names

This guide supports Oracle Communications Session Delivery Manager Version 7.4 and subsequent 7.4 maintenance releases. File names and directories include “xx” to denote the possible presence of alphanumeric characters for maintenance releases. If you are not running a Oracle Communications Session Delivery Manager maintenance release, you can disregard the “xx”.

Below is an example of a file name for releases 7.4 and 7.4M1:

NNC74Linux64bit.tar.gz

Oracle Communications Session Delivery Manager 7.4:

- NNC74Linux64bit.tar.gz

Oracle Communications Session Delivery Manager 7.4M1:

- NNC74M1Linux64bit.tar.gz

---

## Related Session Delivery Manager Documentation

The following table lists related documents for the Oracle Communications Session Delivery Manager

Document Name	Document Description
Release Notes	Contains information about the administration and software configuration of the Oracle Communications Session Delivery Manager feature support new to this release.
Installation Guide	Contains graphical and next mode installation information.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Communications Session Delivery Manager.
High Availability Guide	Describes Oracle Communications Session Delivery Manager High Availability (HA) and the HA cluster, which is a network of tightly-linked servers. HA provides continuous management of the SDM system.
Web Services SOAP XML Provisioning API Guide	Provides a full description of the individual interface definitions that make up the Application Programming Interface (API).
REST API Guide	The OC SDM REST API consists of resources, representations, URIs and HTTP request types that make up the uniform interface used for client/server data transfers.
Core Functionality Guide	Contains an overview of the Oracle Communications Session Delivery Manager graphical user interface

## About this guide

Document Name	Document Description
	(GUI), and detailed information about managing devices and licenses.
Session Element Manager Guide	Contains detailed information pertaining to the Session Element Manager application and describes the dashboard summary view, audit log, fault, and performance views.
Session Route Manager Guide	Contains detailed information about centrally automating the management and distribution of routing data.
Quick Start Guide	Contains a brief description of the GUI, along with information on how to add a device and perform basic configuration tasks.
Administration Guide	Contains information about security administration, which lets you create new users and new user groups, and set group-based authorization.
Application Orchestrator User Guide	Contains detailed information of the use Application Orchestrator to set up and deploy virtual appliances.
Report Manager Installation Guide	Contains instructions for installing Report Manager's dependencies and registering BI Publisher.
Report Manager User Guide	Contains information about configuring collection groups and creating reports.

## Revision History

Date	Description
May 2014	<ul style="list-style-type: none"><li>Initial release</li></ul>
November 2014	<ul style="list-style-type: none"><li>Updates for Release 7.4M2</li></ul>
December 2014	<ul style="list-style-type: none"><li>Adds Troubleshooting Missing Libraries</li></ul>
February 2015	<ul style="list-style-type: none"><li>Removes SSL v3 support from OCSDM</li></ul>
March 2015	<ul style="list-style-type: none"><li>Changes NNC73 to NNC74 in examples</li><li>Changes Net-Net Central to Session Delivery Manager</li></ul>
June 2015	<ul style="list-style-type: none"><li>Removes old reference to RHEL 5.5</li><li>Adds Hazelcast port 54327 to firewall section</li></ul>

---

## Installation Prerequisites

Before installing Oracle Communications Session Delivery Manager:

1. Ensure your system meets the minimum requirements.
2. Open ports on the network and system firewall.
3. Edit the `/etc/hosts` file.
4. Disable the default `httpd` daemon.
5. Install the required dependencies.
6. Setup the `nncentral` group and user account.
7. Unzip the Oracle Communications Session Delivery Manager tar file on your server to create the `AcmePacket` Directory.

## Overview

---

This chapter explains how to install Oracle Communications Session Delivery Manager in a Linux operating system. This release of Oracle Communications Session Delivery Manager supports the following.

## Hardware Support

The Session Delivery Manager supports the following hardware:

- AP 1100
- AP 2600
- AP 3800
- AP 3810
- AP 3820
- AP 4250
- AP 4500
- AP 4600
- AP 6100
- AP 6300
- AP 7000
- AP 7250
- AP 9200
- AP 17350
- AP Enterprise Session Director - Server Edition

## Installation Prerequisites

---

- AP Enterprise Session Director - Virtual Machine Edition

### Trunk Manager Hardware Support

The Trunk Manager application supports the following hardware:

- AP 3800
- AP 4500
- AP Enterprise Session Director - Server Edition
- AP Enterprise Session Director - Virtual Machine Edition

## SBC Support

For a comprehensive list of SBC OS support in this release of Oracle Communications Session Delivery Manager, please consult the Release Notes.

### Limited Support

For the Acme Packet 2600, Oracle Communications Session Delivery Manager supports trap as events and alarms in Fault Management. For performance statistics and configuration management, the Session Delivery Manager will redirect the user to the Acme Packet 2600 onboard GUI.

## Installation Prerequisites


---

Before installing Oracle Communications Session Delivery Manager:

1. Ensure your system meets the minimum requirements.
2. Open ports on the network and system firewall.
3. Edit the `/etc/hosts` file.
4. Disable the default `httpd` daemon.
5. Install the required dependencies.
6. Setup the `nncentral` group and user account.
7. Unzip the Application Orchestrator tar file on your server to create the `AcmePacket` directory.
8. Decide whether to install Oracle's Session Delivery Manager or to install a third-party EMS.

## System Requirements

Oracle has certified the following hardware and software server platforms; and client requirements for use with Oracle Communications Session Delivery Manager Version 7.4.

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

### Platforms Supported

Oracle has certified the following hardware and software platforms, and client requirements for use with Session Delivery Manager Release 7.4:

#### Linux

- CPU: 4-core 2.1 GHz processor or better
- 16 GB RAM minimum, 24 GB RAM recommended
- 195 GB hard drive minimum, 300 GB recommended
- Oracle Linux 6.3 64-bit OVM Template
- Oracle Linux 6.3, 6.4, 6.5 64-bit
- Red Hat Linux 6.3, 6.4, 6.5 64-bit
- CentOS 6.3, 6.4, 6.5 64-bit



### OpenSSL

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 Feb 2013
```

### Client Requirements

- Internet Explorer versions 9.0 and higher or Mozilla Firefox versions 3.0 and higher or Google Chrome versions 23.0 or higher
- Flash player compatible with your browser installed locally
- If the server is not part of your DNS domain, the hosts file on each client must be edited to include the hostname and IP address of the Oracle Communications Session Delivery Manager server. The client host file is usually located in the following directory:

windows\system32\drivers\etc

### Using the DNS Database

All Oracle Communications Session Delivery Manager servers and clients should be configured to use the DNS database for host name lookups. Oracle Communications Session Delivery Manager servers should be defined in the DNS database.

If you are not using the DNS service, you must ensure the hosts file on all Oracle Communications Session Delivery Manager servers and clients contain entries for the Oracle Communications Session Delivery Manager server.

### Information You Need

Ensure that you have identified the following information before you install:

- Hostname and IP address/netmask of the Oracle Communications Session Delivery Manager server, as well as the IP addresses of its gateway, subnet mask, and DNS server
- IP address for each Acme Packet SBC
- SNMP community strings for each Acme Packet SBC

### Components Required

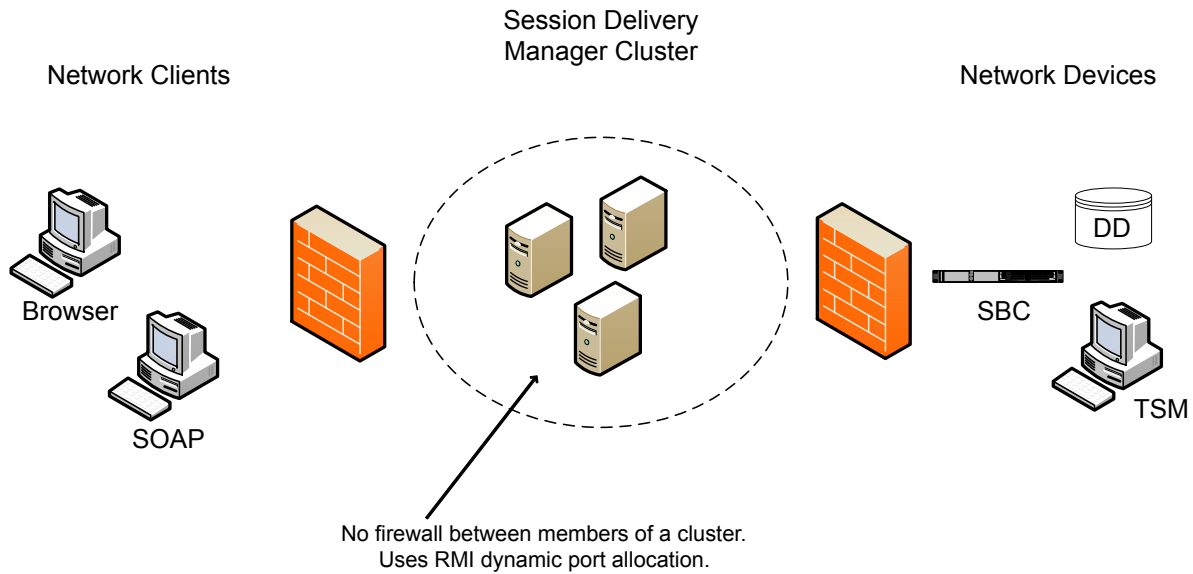
To install Oracle Communications Session Delivery Manager, you need to obtain the appropriate tar.gz file for your environment from your Oracle representative.

- SDM74Linux64bit.tar.gz for Linux RHEL v6.3 64 bit installation
- SDM74RHEL64bit.tar.gz for CentOS 6.3 and CentOS NNC-VM installation

### Firewall Settings

When setting up Oracle Communications Session Delivery Manager in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the Oracle Communications Session Delivery Manager cluster, and a firewall between the Oracle Communications Session Delivery Manager cluster and other devices (SBCs, Data Domain (DD), Terminal Server Manager (TSM)).

## Installation Prerequisites



**Note:** You cannot have firewalls between the servers in a cluster.

If firewalls exist on either side of the Oracle Communications Session Delivery Manager 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 Oracle Communications Session Delivery Manager 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 Oracle Communications Session Delivery Manager Cluster and Network Devices					
161	UDP	SNMP	N	Y	SNMP traffic between the SDM server and the SBC.
162	UDP	SNMP	N	Y	SNMP trap reporting from the SBC to the Oracle Communications Session Delivery Manager server.
22/21	SFTP/FTP				Used for file transfer (such as Route Manager and LRT updates).
8080	HTTP	AMI	N	Y	Used by Oracle Communications Session Delivery Manager to communicate with 9200 devices via AMI.
5060	TCP		N	Y	Used for Oracle Communications Session Delivery Manager Trunk Manager (SIPTX) to communicate with SP-SBC.
3001/ 3000		ACP/ACLI			Used by Oracle Communications Session Delivery Manager to communicate with all

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
					versions of the SBC except for the Acme Packet 9200.
Between Oracle Communications Session Delivery Manager Servers in the Cluster					
1098	TCP	RMI	N	Y	RMI Communication between host members in a cluster.
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.
5801	TCP	Hazelcast	N	Y	Used by the Hazelcast management console port for the Oracle Communications Session Delivery Manager 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 Oracle Communications Session Delivery Manager server.
8009	TCP	Apache	N	Y	Tomcat port.
9000	TCP	Berkeley	N	Y	Berkeley database.
61616	TCP	Apache	N	Y	Message broker.
22	SFTP	ActiveMQ	N	Y	Used to transfer files between Oracle Communications Session Delivery Manager servers.

Either port 8080 (HTTP) or port 8443 (HTTPS) must be open on the firewall, depending on which port you choose between the network client and Oracle Communications Session Delivery Manager server. If installing on a Linux system, the Linux firewall must also have either 8080 (HTTP) or port 8443 (HTTPS) open.



**Note:** Ports are assigned dynamically via Remote Method Invocation (RMI) dynamic port allocation. If you are enabling and configuring iptables/ipf, all traffic must be allowed between servers in the cluster. Communication between clustered Oracle Communications Session Delivery Manager servers must not be restricted.

## Oracle Linux VM

This section contains information about obtaining, installing, and configuring a guest operating system that is required for using Session Deliver Manager in a virtual environment.

You can install Session Delivery Manager as part of a virtual machine (VM) if you want to use a virtual environment for your deployment. You can obtain the OVM template from the Acme Packet customer portal site.

## Installation Prerequisites

---

You can set up the Session Delivery Manager VM using Oracle Virtual Machine Manager. OVM transforms your system's hardware resources -including the CPU, RAM, hard disk and network controller- to create a fully functional virtual environment.

### Before You Start

Review the following information before proceeding to the instructions. You need to set up your host operating system and install OVM, as well as have the necessary information ready for configuration.

### About the OVM Template

The template installs Oracle Linux 6.2 and proceeds to upgrade to 6.4 before Session Delivery Manager installation. The OVM template includes the following components:

- NNC\_OL62\_OVM.tar.gz

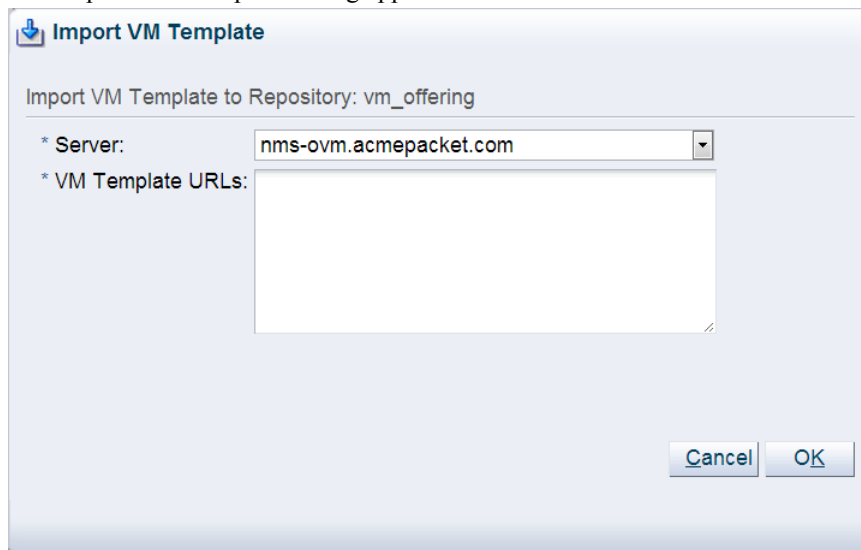
### Memory Usage


Do not provision more virtual memory than you have available in physical memory.

## Deploying the OVM Template

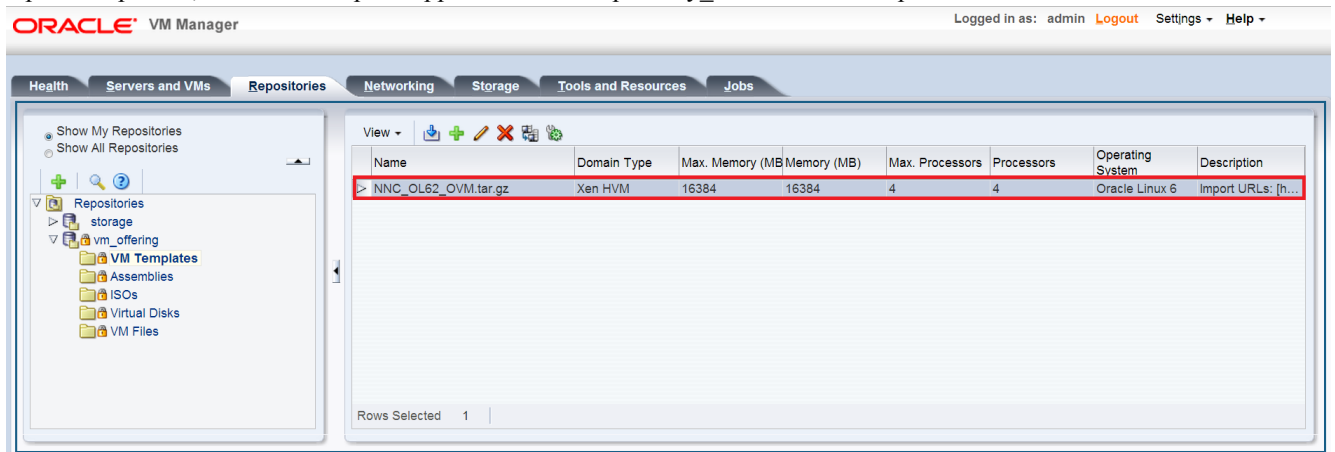
To deploy an OVM template on Oracle VM Manager:

1. Log into the Oracle VM Manager.
2. Click the **Repositories** tab.
3. Select the repository you wish to import the template to and click **Import VM Template**. The Import VM Template dialog appears.



4. Select an OVM server from the drop down list.
5. Enter the VM template's URLs.  
 **Note:** URLs should point to an HTTP or FTP server hosting the OVM template.
6. Click OK to submit the Import VM template request.

Upon completion, the OVM template appears under <Repository\_Name>/VM Templates.



### Creating a Guest VM

To create a guest VM from the OVM template:

1. Click the **Servers and VMs** tab.
2. Click **Create Virtual Machine**.

The Create Virtual Machine dialog appears.

Clone from an existing VM Template

Clone Count: 1

\* Repository: vm\_offering

\* VM Template: NNC\_OL62\_OVM.tar.gz

VM Name: NNC\_OL62\_OVM.tar.gz

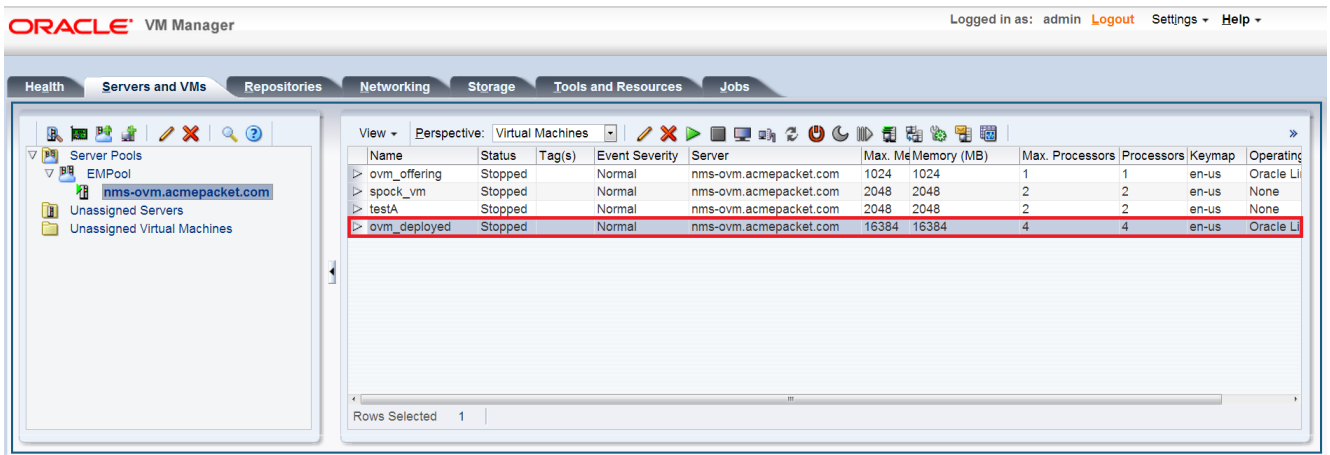
\* Server Pool: EMPool

Description:

3. Select **Clone from an existing VM template**.
4. **Clone Count**—Select the number of desired VMs to create using the up and down arrows.
5. **Repository**—Select the repository holding the OVM template from the drop-down menu.
6. **VM Template**—Select the imported OVM template from the drop-down menu.
7. **VM Name**—Enter a name for the VM you are creating.
8. **Server Pool**—Select a server pool from the drop-down menu.
9. **Description**—Enter an optional description of the VM you are creating.
10. Click **Finish** to create the VM.

The VM is listed on the OVM Server if successfully provisioned.

## Installation Prerequisites

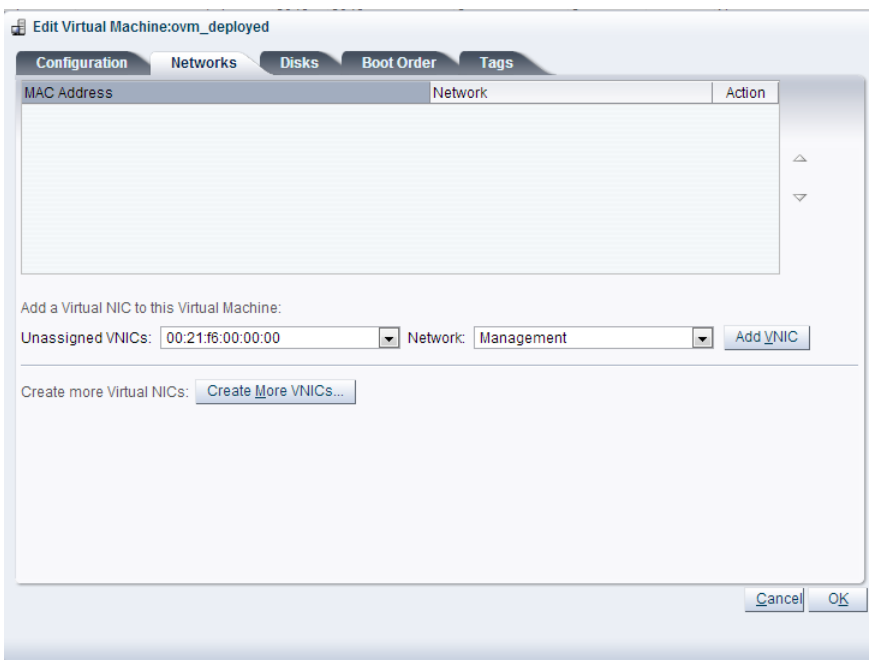


### Adding VNICS to the VM

To add VNICS to your guest VMs:

You must have pre-configured VNICS on the server before you can assign them to the Session Delivery Manager VM. Please consult the documentation for the OVM Manager for information on setting up VNICS on your Network.

1. Select the VM image from the OVM Server table and click the **Edit** button. The Edit Virtual Machine dialog appears.
2. Select the **Networks** tab.



3. **Unassigned VNICS**—Select any VNIC from the drop down list.
4. **Network**—Select the a network for the VNIC from the drop-down menu.
5. Click **Add VNIC** to submit the VNIC configuration. Repeat steps 3-5 to add any remaining unassigned VNICS.
6. Click **OK** to close the Edit Virtual Machine dialog and submit your changes.

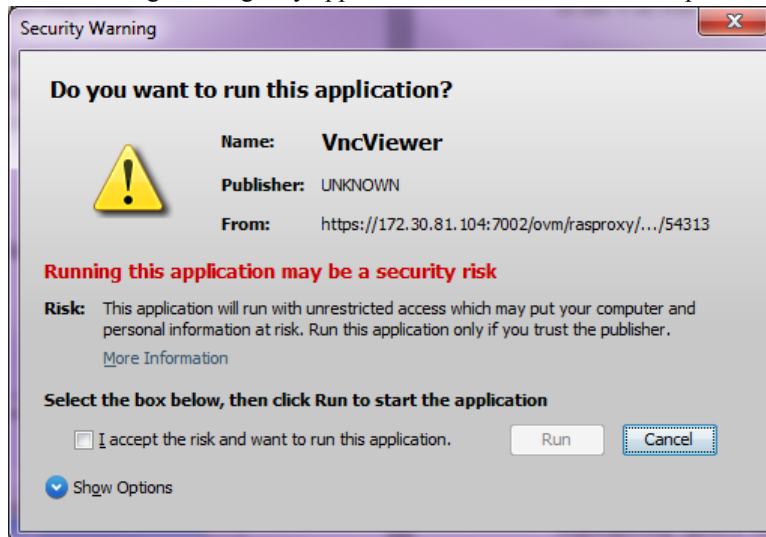
### Launching and Accessing the VM

To launch and access the VM:

1. Select the VM image from the OVM Server table and click the **Play** button.

2. Click the **Start Monitor** button to launch VNC Viewer.
3. Click **Keep** to download the ovm\_rasproxy-ws.jnlp file.
4. Run the ovm\_rasproxy-ws.jnlp file.

The following warning may appear. Click the checkbox to accept and click **Run**.



## Configuring the VM with Sysprep

The sysprep utility guides you through the configuration process for your VM SDM image. If this is your first time installing Session Delivery Manager, you will want to exercise all options in the sysprep utility to fully configure the VM.

1. Log in with the username 'root' and the password 'root123'.

```
localhost login: root
Password: root123

-----

This system is a virtual appliance which has been
prepared by Acme Packet to run Net-Net Central.

Operating system: Oracle Linux 6.2
Acme Packet version: 1.0
-----
=====

First time 'root' login detected.
Running /usr/acme/sysprep.sh

Acme Packet Sysprep will walk you through several
steps needed to configure this system for use as
a Net-Net Central server.
=====
```

2. Enter Y to continue and press <Enter> to launch the sysprep utility.  
Run Acme Packet sysprep utility? (y/n) y

## Changing the root Account Password

For security purposes, you need to change the root account password immediately.

1. Press Enter to accept the default value of 1 to change the root account password.

```
[X] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
```

## Installation Prerequisites

```
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit
```

Please select an option [1] 1

2. Enter Y and press Enter to continue.

```
Change password for account 'root'
Do you wish to continue? (y/n) y
```

3. Enter the new password for the account root and press Enter. You are prompted to confirm the password.

```
New password:
```

4. Enter the password again and press Enter. The confirmation message appears.
5. Press Enter to continue.

### Changing the OS/System Password

1. Select Tools > Passwords and click Update OS/System passwords.  
The Passwords... dialog appears.
2. Select the type of account you would like to update and click OK.  
The Select account dialog appears.
3. Select the user you want to edit and click Update.  
New password and Confirm new password fields appear in the dialog.
4. Enter the new password twice and click Update.  
A confirmation dialog appears.
5. Click Yes to confirm you changes.  
A dialog appears with a success or error message.

### Configuring Networking

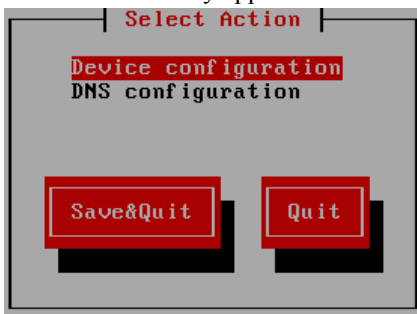
You can configure the ethernet interfaces to use the IP addresses of your network with the following steps.

1. Press <Enter> to accept the default value of 3 to configure networking.

```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[X] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit
```

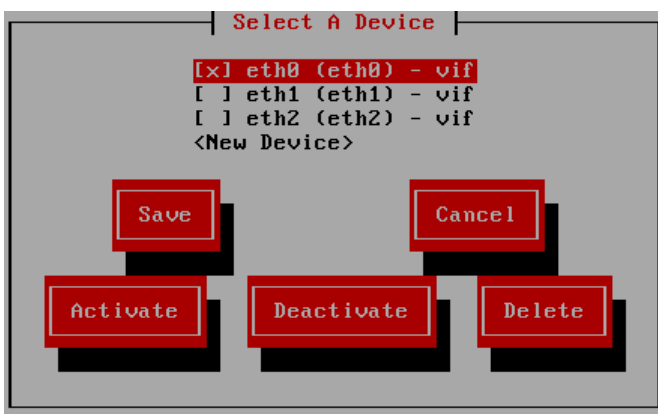
Please select an option [3] 3

2. Enter Y and press <Enter> to continue.  
The Network utility appears.




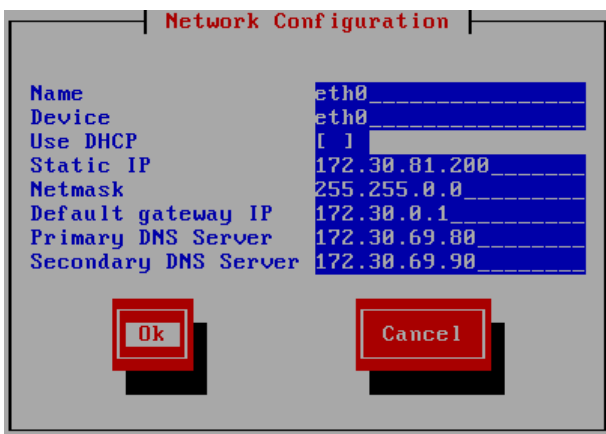
3. Select Device configuration and press <Enter>.  
The device selection dialog appears.






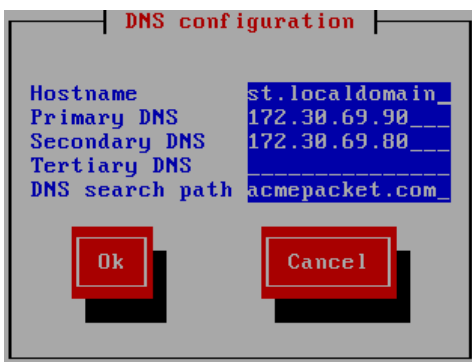
4. Select eth0 and press <Enter>
5. Set the network configuration parameters by using the up and down arrows to reach individual values. Press <Enter> with Ok selected once you are finished.

 **Note:** Acme Packet recommends that users set up eth0 with a static IP address. DHCP is not recommended on eth0.



6. Select Save and press <Enter>.
7. Select DNS configuration and press <Enter>.
8. Set the DNS configuration parameters by using the up and down arrows to reach individual values. Press <Enter> with Ok selected when you are finished.

 **Note:** The system Hostname must be a Fully Qualified Domain Name (FQDN). For example: nnc-vm.acmepacket.com



9. Select Save & Quit and press <Enter>.

## Installation Prerequisites

---

### Configuring the Timezone

You need to select the timezone that the VM is operating in.

1. Press <Enter> to accept the default value of 4 to configure the timezone. You are prompted about continuing.

```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[X] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit
```

Please select an option [4] 4

2. Enter Y and press <Enter> to continue.

The configure timezone utility appears.

3. Enter the corresponding number of the continent or ocean the system is located and press <Enter>.

```
Please select a continent or ocean.
1) Africa                4) Arctic Ocean          7) Australia
10) Pacific Ocean
2) Americas              5) Asia                      8)
Europe
3) Antarctica 6) Atlantic Ocean 9) Indian Ocean
```

4. Enter the corresponding number of the country the system is located and press <Enter>.
5. Enter the corresponding number of the time zone region the system is located and press <Enter>.
6. Enter 1 to confirm the selected timezone and press <Enter> to continue.

```
Therefore TZ='America/New_York' will be used.
Local time is now: Tue Nov 20 12:35:36 EST 2012.
Universal Time is now: Tue Nov 20 17:35:36 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
```

### Configuring the Network Time Protocol

1. Press <Enter> to accept the default value of 5 to configure optional services.

```
[ ] 1. Change root password
[ ] 2. Change nncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[X] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[ ] 7. Exit
```

Please select an option [5] 5

2. Enter Y and press <Enter> to continue.

3. Enter Y and press <Enter> to enable the Network Time Protocol. A list of currently defined NTP servers appears.

```
Enabling Network Time Protocol is recommended
Enable Network Time Protocol (NTP)? (y/n) y
```

4. Enter Y and press <Enter> to include the selected NTP server or N to remove it from the NTP configuration.

```
3 NTP servers are currently defined in /etc/ntp.conf
Use NTP server '0.centos.pool.ntp.org'? (y/n) n
Use NTP server '1.centos.pool.ntp.org'? (y/n) n
Use NTP server '2.centos.pool.ntp.org'? (y/n) n
```

5. Enter Y and press <Enter> to add an additional NTP server. Otherwise, enter N and press <Enter> to continue without adding a new server.

```
Add additional NTP servers
Add NTP server (y/n)
```

6. Enter the IP address or DNS name for the additional NTP server and press <Enter>. The Add additional NTP Servers dialog appears again so you can continue adding other values.

```
Enter IP address or DNS name for NTP server: 192.168.1.101
Added NTP server '192.168.1.101' to /etc/ntp.conf
```

7. Enter N and press <Enter> when you are finished adding NTP servers to your configuration.

```
Add NTP server? (y/n) n
Starting ntpd service...
```

8. Press <Enter> to continue.

### Configuring Optional Services

You must configure optional services if you wish to enable telnet and ftp.

1. Press <Enter> to accept the default value of 6 to configure optional services.

```
[ ] 1. Change root password
[ ] 2. Change ncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[X] 6. Configure optional services
[ ] 7. Exit
```

```
Please select an option [5] 5
```

2. Enter Y and press <Enter> to continue. The configure optional services prompt appears.
3. Enter Y and press <Enter> to enable telnet. Otherwise, enter N and press <Enter> to continue with telnet disabled.

```
Would you like to enable telnet? (y/n)
Enabling telnet...
```

4. Enter Y and press <Enter> to enable FTP. Otherwise, enter Y and press <Enter> to continue with FTP disabled.

```
Would you like to enable ftp?
Enabling ftp...
Updating selinux ftp policy...
```

5. Press <Enter> to continue.

### Exiting Sysprep

To exit the sysprep configuration:

1. Press <Enter> to accept the default value of 6 to configure optional services.

```
[ ] 1. Change root password
[ ] 2. Change ncentral password
[ ] 3. Configure networking
[ ] 4. Configure Timezone
[ ] 5. Configure Network Time Protocol
[ ] 6. Configure optional services
[X] 7. Exit
```

```
Please select an option [7] 7
```

2. Enter Y and press <Enter> to complete the sysprep configuration and reboot the system.



**Note:** Rebooting is required to apply configuration changes.


### Installing Session Delivery Manager

You are able to install Oracle Communications Session Delivery Manager using the typical or custom installation process.

### Before a New Installation

---

This section explains how to configure your operating system before you install Oracle Communications Session Delivery Manager for the first time.

 **Note:** You do not have to complete this process if you are using the NNC-VM. Linux is configured automatically using the sysprep utility as part of the NNC-VM installation process.

### Configuring Linux

To configure Linux:

- Include the Linux host name
- Disable the default http daemon

#### Including the Linux Hostname

You must configure the Linux system hostname during the installation of the operating system. You can determine the hostname by using the hostname command on the Linux system. For example:

```
[bash]$ hostname
nncsvr
```

You need to edit the /etc/hosts file to include the Linux system hostname in the following format:

<IP address>	<hostname>	<hostname>.localdomain
--------------	------------	------------------------

The following example shows the inclusion of a server named nncsvr with an IP address of 10.0.0.252:

```
[bash]$ cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1    localhost    localhost.localdomain
10.0.0.252  nncsvr      nncsvr.localdomain
```

#### Disabling the Default HTTP Daemon

You need to disable the default http daemon process on the Oracle Communications Session Delivery Manager server.

To disable the http daemon:

1. Log in as root user and open a Terminal window.
2. Stop the httpd daemon if it is running:

```
sbin/service httpd stop
```

3. Disable the http daemon from restarting a system reboot:

```
chkconfig httpd off
```

4. Verify the httpd daemon is not running:

```
sbin/service httpd status
```

The following message appears:

```
httpd is stopped
```

#### Setting the System Locale

You must set the system locale to en\_US.UTF-8 in order for Oracle Communications Session Delivery Manager to install properly.

To set the locale:

1. Log in as root.

2. Run the following command to set the locale to en\_US.UTF-8:

```
export LC_ALL=en_US.UTF-8
```

### Displaying Shared Libraries

You need to display the shared libraries and check that they are connected. If any libraries are not connected, you can create soft links for them. For example, in Fedora Core 13 you might need to create soft links for two libraries.

To display shared libraries:

1. As root user, change to the httpserver bin directory. For example:

```
cd /opt/AcmePacket/NNC74/Apache/httpserver/bin
```

2. Run the following command to display the shared libraries:

```
ldd httpd
```

Output similar to the following for Fedora Core 13 appears:

```
linux-vdso.so.1 => (0x00007fff9e8b0000)
libm.so.6 => /lib64/libm.so.6 (0x0000003b7f400000)
libaprutil-1.so.0 => /usr/lib64/libaprutil-1.so.0 (0x00007f85607ea000)
libexpat.so.0 => (file not found)
libuuid.so.1 => /lib64/libuuid.so.1 (0x0000003b83800000)
librt.so.1 => /lib64/librt.so.1 (0x0000003b80400000)
libcrypt.so.1 => /lib64/libcrypt.so.1 (0x0000003b8fe00000)
libpthread.so.0 => /lib64/libpthread.so.0 (0x0000003b7fc00000)
libdl.so.2 => /lib64/libdl.so.2 (0x0000003b7f800000)
libc.so.6 => /lib64/libc.so.6 (0x0000003b7f000000)
libdb-4.8.so => /lib64/libdb-4.8.so (0x0000003b95200000)
/lib64/ld-linux-x86-64.so.2 (0x0000003b7e800000)
libfreebl3.so => /lib64/libfreebl3.so (0x0000003b90200000)
```

One of the shared libraries libexpat.so.0 is not found. A soft link must be created for it.

### Creating Soft Links

You can create soft links for any shared libraries that are not connected.

To create soft links:

1. As root user, change directory to /usr/lib64.
2. Create links for any unlinked shared libraries. For example:

```
ln -s libexpat.so.1.5.2 libexpat.so.0
ln -s libexpat.so.1.5.2 ../../lib64/libexpat.so.0
```

## User and Group Accounts

For security reasons, you must create a user account named nncentral and a group named nncentral. You also must define 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 nncentral. The main Oracle Communications Session Delivery Manager process has to run as a sudo user in order to have access to port 162.

### Creating nncentral Group and User

To create nncentral group and user:

1. Login as root.
2. Enter the following lines:


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


## Installation Prerequisites

---

### Edit the sudoer Configuration File

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

 **Note:** This file can only be edited using vi editor commands.


 **Note:** Press i to enter insert mode and begin adding text. Press Esc to return to command mode.


1. Log in as root.
2. Execute visudo.

```
# visudo
```

3. Add the following line to the sudoer configuration:

```
nncentral ALL=/opt/AcmePacket/NNC*/jre/bin/java * -Dlog4j.configuration=* -  
cp * com.acmepacket.ems.server.services.snmp.TrapRelay.TrapRelay *
```

 **Note:** In command mode, press :wq to save your changes and exit visudo.

 **Note:** In command mode, press :q! to quit without saving your changes.

## Installing Oracle Communications Session Delivery Manager

---


This section explains how to install and setup Oracle Communications Session Delivery Manager on the Oracle Communications Session Delivery Manager server. The steps are the same for all supported operating systems.

To install Oracle Communications Session Delivery Manager, you need to obtain the appropriate tar.gz file for your environment. You explode the tar file contents on your server and run the setup script to configure Oracle Communications Session Delivery Manager.

### Installing Oracle Communications Session Delivery Manager

To install Oracle Communications Session Delivery Manager:

1. Obtain the appropriate tar.gz file from the Oracle customer portal.
2. FTP the tar.gz file to your system. Place the file in the directory where you want the Oracle Communications Session Delivery Manager software to reside after you unzip the tar.gz file. For example, FTP the tar file to the /opt directory.

 **Note:** You cannot install an older version of Oracle Communications Session Delivery Manager in the same directory as a newer version.

3. Unzip the \*.tar.gz file.

```
gunzip <filename>.tar.gz
```

4. Extract the files using one of the following commands:

```
tar -xvf <filename>.tar
```

From here you run setup to configure Oracle Communications Session Delivery Manager.

### Running Setup

The following steps show running setup on a Linux system.

To run setup:

1. Login as root user.
2. Navigate to the bin directory. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Run setup.sh.

```
./setup.sh
```

A Welcome message appears and initialization processes occur. Setup checks that minimal system requirements are met and checks system port availability for Oracle Communications Session Delivery Manager components.

This process may take several minutes to complete. Do not kill the setup.sh process during this time or you will risk corrupting the system.

```
[root@nms-vm4 opt]# cd AcmePacket/NNC74/bin/
[root@nms-vm4 bin]# ./setup.sh
```

```
=====
Welcome to Oracle Communications Session Delivery Manager Setup application
Version : NNC74
OS : Linux : amd64 : 2.6.18-274.12.1.el5
=====
```

```
Please wait while application loads
Checking environment and setting permissions.
Please wait ....
The process may take some time to complete dependent on the system. Please
do NOT interrupt or exit this application, otherwise it might compromise
the setup environment!
100%[=====]
```

```
=====
System Physical Memory Diagnostics
Total System Physical Memory = 16384 MB
Total System Free Physical Memory = 15057 MB
Dynamic memory allocation in progress
Previous database cache 262144000
New database cache 2907701248
Previous JVM Xmx size 1024
New JVM Xmx size 8092
=====
```

```
System Disk Space Diagnostics
Total System Disk Space = 127 GB
Free System Disk Space = 117 GB
WARNING: Disk space is insufficient for running this application.
The recommended total disk space that should be available is = 300 GB
=====
```

```
System Port Availability Diagnostics : OC SDM Required Ports
The following port is available [ 5000 ]
The following port is available [ 8080 ]
The following port is available [ 61616 ]
The following port is available [ 9000 ]
The following port is available [ 5432 ]
The following port is available [ 8443 ]
The following port is available [ 1099 ]
The following port is available [ 8009 ]
The following port is available [ 1098 ]
The following port is available [ 8005 ]
```

```
Configuring Postgres. This may take several minutes.
Please wait. Done!
=====
```

## Installation Prerequisites



**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.

After the diagnostics, the setup options appear.

```
Set up options
TYPICAL      : This setup procedure walks the user through the
               minimal setup configuration required to configure
               OC SDM server.
CUSTOM       : This setup procedure provides the user with
               a set of options to manually pick and
               choose from.

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

Please select an option [1]
```

Choose the Typical setup option if you are new to Oracle Communications Session Delivery Manager or just want to create the minimal configuration required by the Oracle Communications Session Delivery Manager server. Choose Custom if you are a more advanced user or are licensed for applications hosted on Oracle Communications Session Delivery Manager. The Custom setup also includes the options available on the Typical setup.

You can run the setup repeatedly to change existing configuration values and to access any new Custom options as a result of licensing additional applications.

## Typical Setup

The Typical setup performs the minimal configuration required by the Oracle Communications Session Delivery Manager server in order to run properly. If this is your first time installing Oracle Communications Session Delivery Manager, you will need to exercise all options in the Typical Setup to fully configure the Oracle Communications Session Delivery Manager server.

To perform a typical setup:

1. Press Enter to accept the default value 1 for a typical setup. You are prompted to continue.
2. Enter Y and press Enter to continue. The list of Typical configuration options appears.

```
Typical Configuration
Will walk through basic configuration options.

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

Please select an option [1]
```

3. Verify with your system administrator that you have the correct sudo password before continuing.

## Configure Default User Account Passwords

You need to configure default passwords for the admin and Lladmin 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 - OC SDM global identifier configuration
[ ] 3 - HTTP/HTTPS configuration
[ ] 4 - Fault Management configuration
[ ] 5 - Quit setup
```

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

### Global Identifier Configuration During Installation

To configure global identifiers from the typical and custom installation procedures:

1. Press <Enter> to accept the default value of 2. You are prompted about continuing..

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

Please select an option [2]

2. Enter Y and press <Enter> to continue.
3. Enter a global unique identifier for the system.


```
OC SDM global identifier configuration
This option allows the end user to specify a unique global identifier for
installing cluster or standalone OC SDM in user's deployment environment.
(if this installation is for cluster environment, you need to use the same
global identifier on all cluster nodes)

Global identifier
Enter global identifier: [OCSDM] SDM1
```

4. Press <Enter> to submit and continue with the installation procedure.

### HTTP

To configure HTTP mode:

 **Note:** You cannot use the value root for either the user or group name.

1. Press **Enter** to accept the default value of 3. You are prompted about continuing.

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

Please select an option [3]

Do you want to continue Yes/No?

2. Enter Y and press Enter to continue. The HTTP/HTTPS options appear.

Do you want to continue Yes/No?y

HTTP/HTTPS configuration

## Installation Prerequisites

```
Set up HTTP or HTTPS configuration
[X] 1 - HTTP mode - Configure server to run in HTTP mode   [Default]
[ ] 2 - HTTPS mode - Configure server to run in HTTPS mode
```

```
Please select an option [1]
```

3. Press Enter to accept the default to configure HTTP. You are prompted about continuing.
4. Enter Y and press Enter to continue. You are prompted for the username of the server process.

```
Do you want to continue Yes/No?y
```

```
HTTP mode
Configure server to run in HTTP mode
```

```
Enter the user name of the server process which determines what files the
server is allowed to access. Any files inaccessible to this user are also
inaccessible to clients connecting to the Apache HTTP Server.
Apache User [nncentral]
```


5. Press Enter to accept the default value nncentral. You are prompted for the group name.

```
Enter the group name of the Apache HTTP Server processes
Apache Group [nncentral]
```

6. Press Enter to accept the default value nncentral. You are prompted for the port number.

```
Enter the port number that the Apache HTTP Server should listen on
Apache Port Number (1024-65535) [8080]
```

7. Press Enter to accept the default value 8080. The list of Typical setup options appears.

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

```
[ ] 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
```

```
Please select an option [4]
```

## HTTPS

To configure HTTPS mode:

1. Enter 2 to configure HTTPS and press Enter. You are prompted about continuing.

```
Please select an option [1] 2
```

```
[ ] 1 - HTTP mode - Configure server to run in HTTP mode   [Default]
[X] 2 - HTTPS mode - Configure server to run in HTTPS mode
```

```
Do you want to continue Yes/No?
```

2. Enter Y and press Enter to continue. You are prompted for the user name for the server process.


```
HTTPS mode
Configure server to run in HTTPS mode
```

```
Enter the user name of the server process which determines what files the
server is allowed to access. Any files inaccessible to this user are also
inaccessible to clients connecting to the Apache HTTP Server.
Apache User [nncentral]
```

3. Press Enter to retain the default nncentral. You are prompted for the group name.

```
Enter the group name of the Apache HTTP Server processes
Apache Group [nncentral]
```

4. Press Enter to retain the default nncentral. You are prompted for the port number the server should listen on.

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

```
Enter the port number that the Apache HTTP Server should listen on
Apache Port Number (1024-65535) [8443]
```

5. Press Enter to retain the default 8443. You are prompted for the server's DNS name.

```
The server name(DNS name of this server)
Server name []
```

6. Enter the DNS name of the server and press Enter. You are prompted about creating a self-signed certificate.

 **Note:** Skip to [Creating Self-Signed Certificate](#) to create a self-signed certificate.

```
Would you like to create a self signed certificate?
[ ] 1 - Yes
[X] 2 - No    [Default]

Please select an option [2]
```

### No Self-Signed Certificate

1. Retain the default value No if you do not want to create a self-signed certificate.
2. Press Enter. You are prompted about continuing.

```
[ ] 1 - Yes
[X] 2 - No    [Default]
```

```
Do you want to continue Yes/No?y
```

3. Enter Y to continue and press Enter. You are prompted for the private key file.

```
Do you want to continue Yes/No?y
```

```
The private key file
Private key file []
```

4. Enter the file name, including the path, and press Enter. You are prompted for the certificate file.
5. Enter the file name, including the path, and press Enter. You are prompted about intermediate certificates.
6. Press Enter to accept the default. You are prompted about continuing.
7. Enter Yes to continue. You are prompted for the alias name for the certificate in the truststore.
8. Press Enter to accept the default or enter a different alias name and press Enter. You are prompted for the trustore password.
9. Press Enter to accept the default or enter a different password and press Enter.

### Creating Self-Signed Certificate

To create a self-signed certificate:

1. Enter 1 if you want to create a self-signed certificate and press Enter. You are prompted about continuing.

```
Please select an option [2]1

[X] 1 - Yes
[ ] 2 - No    [Default]
```

2. Enter Y to continue and press Enter. You are prompted for the common name (DNS name) of the server.
3. Enter the DNS name of the server and press Enter. You are prompted for the certificate alias name in the trustore.

## Installation Prerequisites

---

4. Retain the default or enter a different alias name and press Enter. You are prompted for the trustore password.
5. Enter the trustore password and press Enter. The Typical install list of options appears.

```
[ ] 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

Please select an option [4]
```

From here you configure fault management.



**Note:** Verify with your system administrator that you have the correct sudo password before continuing.

### 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]
```



**Note:** If you enter a port below 1024, Oracle Communications Session Delivery Manager prompts you for the sudo password.

4. If prompted, enter the sudo password. Then re-enter the sudo password to confirm.
5. Select option 5, **Quit setup**. Press Enter to continue.

### Configuring the sudo Password

Oracle Communications Session Delivery Manager requires the sudo password to configure Trap Relay on ports 1024 and under. You set the sudo password to match the sudo password that has been defined by the system administrator. Installation automatically skips these steps if you select a port 1025 or higher.

To configure a sudo password:

1. You are prompted for the sudo password.

```
OC SDM requires entry of the sudo password in order to
support internal components that require sudo user privileges.
The password you supply will be securely encrypted.
```

```
Enter sudo password: []
```

Enter the sudo password for user account ncentral and press Enter. You are prompted to confirm the password.

2. Enter the password again and press Enter. The confirmation message appears.

```

Confirm sudo password: []
Sudo password entered and encrypted successfully!

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


Please select an option [5]

```

## Custom Installation

The custom installation options are for more advanced users. These options include:

- Mail server configuration
- OC SDM cluster management
- Route Manager configuration
- SAML Single Sign On configuration
- SBI TLS configuration
- Oracle Database configuration

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

## Accessing Custom Options

The following instructions are based on configuring setup options on a Linux system.

To access custom setup options:


1. Login as root user.
2. Navigate to the bin directory. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Run setup.sh.

```
./setup.sh
```

A Welcome message appears and initialization processes occur. Setup checks that minimal system requirements are met and checks system port availability for Oracle Communications Session Delivery Manager components.

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

After the diagnostics, the setup options appear.

```

Set up options
TYPICAL   : This setup procedure walks the user through
            the minimal setup configuration required to
            configure Net-Net server.
CUSTOM    : This setup procedure provides the user with
            a set of options to manually pick and
            choose from.

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

```

## Installation Prerequisites

---

```
Please select an option [1] 2
```

4. Enter 2 for Custom and press Enter. You are prompted about continuing.
5. Enter Y and press Enter. The custom setup options appear.

```
[ ] 1 - Typical : Runs through most common set up options.
[X] 2 - Custom : Allows manual customization.
[ ] 3 - Check : Finish and quit setup.
Do you want to continue Yes/No?Y
=====
[X] 1 - Check and Apply License [Default]
[ ] 2 - OC SDM global identifier configuration
[ ] 3 - HTTP/HTTPS configuration
[ ] 4 - Fault Management configuration
[ ] 5 - Mail Server configuration
[ ] 6 - OC SDM cluster management
[ ] 7 - Route Manager Central configuration
[ ] 8 - SAML Single sign on configuration
[ ] 9 - Trunk Manager configuration
[ ] 10 - SBI TLS configuration
[ ] 11 - Quit setup
Please select an option [1] 1
```

See the information in Typical Setup for details about the following options:

- Check and Apply License
- HTTP/HTTPS configuration
- Fault Management configuration

See the following sections for details about the custom options.

## Mail Server

The Mail server setup option is visible even if you are not licensed for Element Manager or Report Manager. If you are licensed for Report Manager, you can setup the mail server credentials to enable the sending of emails to a targeted Microsoft Exchange and Gmail server.

To configure the mail server:

1. Press Enter to accept the default of 5 for Mail Server configuration setup. You are prompted about continuing.

```
=====
[ ] 1 - Check and Apply License [Default]
[ ] 2 - OC SDM global identifier configuration
[ ] 3 - HTTP/HTTPS configuration
[ ] 4 - Fault Management configuration
[X] 5 - Mail Server configuration
[ ] 6 - OC SDM cluster management
[ ] 7 - Route Manager Central configuration
[ ] 8 - SAML Single sign on configuration
[ ] 9 - Trunk Manager configuration
[ ] 10 - SBI TLS configuration
[ ] 11 - Quit setup
Please select an option [1] 1
```

2. Enter Y and press Enter. The mail server configuration options appear.

```
Mail Server configuration
This option is used to configure mail server
Configure mail server
Mail server configuration can be used for trap notification.
Please choose to quit mail server configuration or apply new configuration
[X] 1 - Configure mail server [Default]
```

```
[ ] 2 - Quit out of mail server configuration
Please select an option [1]
```

3. Press Enter to configure the mail server. You are prompted to continue.
4. Enter Y and press Enter to continue. The status of the mail server indicates it is not configured and the mail server host options appear.

```
Do you want to continue Yes/No?
Mail server: Not configured
```

```
Use the following options to configure mail server host.
[X] 1 - Configure mail server host
[] 2 - Apply new mail server configuration [Default]
[] 3 - Cancel out and do not apply changes
```

```
Please select an option [1]
```

5. Press Enter to configure the mail server host. You are prompted to continue.
6. Enter Y to continue. You are prompted for the server DNS name.

```
Do you want to continue Yes/No?Y
Mail server: Not configured
```

```
Provide the DNS name.
Host name [ ]
```

7. Enter the DNS name and press Enter. For example, mail.acmepacket.com. If configuring a Gmail server you might enter smtp.gmail.com. The mail server name is changed and the mail server configuration options appear.

```
Do you want to continue Yes/No?Y
Mail server: Not configured
```

```
Provide the DNS name.
Host name [ ] mail.acmepacket.com
Mail server host name has been changed
Mail from: Not configured
```

```
Use the following options to configure mail from.
[X] 1 - Configure mail from
[] 2 - Apply new mail server configuration
[] 3 - Cancel out and do not apply changes [Default]
```

```
Please select an option [1]
```

8. Press Enter to configure the From address you want to use. You are prompted about continuing.
9. Enter Y and press Enter to continue. You are prompted for the mail from address.
10. Enter the address you want used for the From address and press Enter. For example, if sending to Microsoft Exchange account mailadmin@acmepacket.com. If sending to a Gmail account, mailadmin@gmail.com. You are prompted about the mail server properties.

```
Provide the mail from.
Mail from [ ] mailadmin@acmepacket.com
Mail from has been changed
Mail server propertiesNot configured
Configure Mail server properties
[X] 1 - Configure Mail server properties
[] 2 - Apply new mail server configuration
[] 3 - Cancel out and do not apply changes [Default]
Please select an option [1]
```

11. Press Enter to configure mail properties. You are prompted about continuing.
12. Enter Y and press Enter to continue.
13. Enter the mail server properties for your mail server.

## Installation Prerequisites

---

```
Do you want to continue Yes/No?
Mail server propertiesNot configured
Provide the server properties if needed.
Mail server properties [ ] mail.smtp.starttls.enable:true
Mail server properties have been changed
Mail logon required: Not configured
```



**Note:** The format for entering multiple mail server properties is:

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

14. Press Enter to continue. You are prompted whether to configure whether the mail logon is required.

15. Press Enter if logon is not required. Or enter true and press Enter. If false, the mail server host configuration options appear. If true, the mail logon user configuration options appear.

```
Provide the mail logon required.
Mail logon required true/false [false] true
Mail logon required has been changed
Mail logon user: Not configured

Use the following options to configure mail logon user.
[X] 1 - Configure mail logon user
[ ] 2 - Apply new mail server configuration
[ ] 3 - Cancel out and do not apply changes [Default]
```

```
Please select an option [1] █
```

16. Press Enter to configure the mail logon user. You are prompted about continuing.

17. Enter Y and press Enter to continue. You are prompted for the mail logon user.

18. Enter the username and press Enter. For example, if sending to a Microsoft Exchange server mailrecipient@acmepacket.com. Or for Gmail, mailrecipient@gmail.com. The mail logon user status changes and the configuration options appear.

```
Do you want to continue Yes/No?Y
Mail logon user: Not configured

Provide the mail logon user.
Mail logon user [ ] mailrecipient@acmepacket.com
Mail logon user has been changed
Mail logon user password: Not configured

Use the following options to configure mail logon user password.
[X] 1 - Configure mail logon user password
[ ] 2 - Apply new mail server configuration
[ ] 3 - Cancel out and do not apply changes [Default]
```

```
Please select an option [1] █
```

19. Press Enter to configure the mail logon user password. You are prompted about continuing.

20. Enter Y to continue and press Enter. You are prompted for the password.

21. Enter the password the user enters when they logon and press Enter. (Nothing displays on the screen when you enter the password.) The logon user password status changes and the configure mail server host options appears.



```

Do you want to continue Yes/No?
Mail logon user password: Not configured

Provide the mail logon user password.
Mail logon user password [ ]
Mail logon user password has been changed
Mail server: abc

Use the following options to configure mail server host.
[ ] 1 - Configure mail server host
[X] 2 - Apply new mail server configuration [Default]
[ ] 3 - Cancel out and do not apply changes
    
```

Please select an option [2]

22. You can cancel the configuration without applying the changes or press Enter to apply the changes to the mail server configuration. You are prompted about continuing.

23. Enter Y to continue and press Enter. You are prompted to either apply the new configuration or quit.


```

Please choose to quit mail server configuration or apply new configuration
[X] 1 - Configure mail server [Default]
[ ] 2 - Quit out of mail server configuration
Please select an option [1] 2
[ ] 1 - Configure mail server [Default]
[X] 2 - Quit out of mail server configuration
    
```

24. Press Enter to quit the mail server configuration. You are asked if you wish to continue.

## Cluster Management

If you are licensed for Element Manager, the Oracle Communications Session Delivery Manager cluster management option appears. Access this option to configure and manage a cluster of Oracle Communications Session Delivery Manager servers for High Availability (HA). See the Oracle Communications Session Delivery Manager High Availability Guide for more information about HA and clusters.

 **Note:** Ensure you synchronize time on each server with NTP before adding it to a cluster.

To configure clusters:

1. Enter 6 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter. The cluster management options appear.

```

Do you want to continue Yes/No?Y

=====

Net-Net Central cluster management.
This option is used to configure NNC as part of a cluster

Management options
The host machine can run as a standalone or member of a Net-Net Central cluster.

Please choose to quit cluster management or apply new configuration
[X] 1 - Configure and manage members in cluster [Default]
[ ] 2 - Run current host as a standalone
[ ] 3 - Quit out of cluster configuration

Please select an option [1] █
    
```

### Manage Cluster Members

1. Press Enter to configure and manage members in a cluster. You are prompted about continuing.
2. Enter Yes and press Enter. The cluster member management options appear.

```
Host name          | DB      | MOM      | Web Worker
                   | Port    | Port     | Port
localhost          | 9000    | 61616    | 8009
```

Use the following options to add or remove members from cluster.

```
[ ] 1 - Add a new member
[ ] 2 - Remove all remote members
[ ] 3 - Apply new cluster configuration
[X] 4 - Cancel out and do not apply changes [Default]
```

### Adding New Members

To add new member to a cluster:

1. Enter I and press Enter. You are prompted about continuing.
2. Enter Y and press Enter. You are prompted for the IP address of the host you want to add.

```
Do you want to continue Yes/No?Y
Host name          | DB      | MOM      | Web Worker
                   | Port    | Port     | Port
localhost          | 9000    | 61616    | 8009
Provide the IP address of the Host requiring membership to the cluster.
Member host name [ ]
```

3. Enter the IP address for the host you are adding to the cluster and press Enter. A confirmation message appears and the options appear again.

```
Provide the IP address of the Host requiring membership to the cluster.
Member host name [ ]172.30.80.19
Valid remote member has been added
Host name          | DB      | MOM      | Web Worker
                   | Port    | Port     | Port
localhost          | 9000    | 61616    | 8009
===== Remote members =====
172.1.30.185       | 9000    | 61616    | 8009
172.30.80.19       | 9000    | 61616    | 8009
Use the following options to add or remove members from cluster.
[ ] 1 - Add a new member
[ ] 2 -
[X] 3 - Apply new cluster configuration
[ ] 4 - Cancel out and do not apply changes [Default]
```

4. Repeat steps to add additional hosts to the cluster. When you are done adding hosts to the cluster you can apply the new cluster configuration.
5. Press Enter to accept the default 3 Apply new cluster configuration. (Or you can cancel out of creating a cluster without applying your changes.) You are prompted about continuing.
6. Enter Yes and press Enter. The cluster members are displayed and the cluster management options appear.

```

Do you want to continue Yes/No?Y
Host name          | DB      | MOM     | Web Worker
                   | Port   | Port   | Port
172.30.1.185      | 9000   | 61616  | 8009

===== Remote members =====
172.30.80.19      | 9000   | 61616  | 8009
172.30.80.9       | 9000   | 61616  | 8009
172.30.80.198    | 9000   | 61616  | 8009

Please choose to quit cluster management or apply new configuration
[X] 1 - Configure and manage members in cluster  [Default]
[ ] 2 - Run current host as a standalone
[ ] 3 - Quit out of cluster configuration

```

Please select an option [1] █

7. Enter 3 and press Enter to quit out of the cluster configuration. You are prompted about continuing.
8. Enter Y and press Enter. The Configure sftp information options appear and your are prompted about your host being a member of a Oracle Communications Session Delivery Manager cluster.

Please select an option [1] 3

```

[ ] 1 - Configure and manage members in cluster  [Default]
[ ] 2 - Run current host as a standalone
[X] 3 - Quit out of cluster configuration

```

Do you want to continue Yes/No?Y

Configure sftp information  
 Make sure to configure sftp properties if there are members in the cluster

```

Will this machine be a member of a Net-Net Central cluster?
[ ] 1 - Yes
[X] 2 - No  [Default]

```

Please select an option [2] □

9. Press Enter to retain the default value No or enter 1 to add your current host to the cluster. See the following section for instructions.

### Adding Current Host to Cluster

You can include the host on which you are running setup in the cluster.

1. Enter Y to continue when prompted. A prompt appears for the username to use to SFTP files from the host.

Please select an option [2] 1

```

[X] 1 - Yes
[ ] 2 - No  [Default]

```

Do you want to continue Yes/No?Y

Please enter the username to use to sftp files off of this machine  
 Username [ ] □

2. Enter the username you want to use to SFTP files and press Enter. You are prompted for the password.
3. Enter the password to use to SFTP files and press Enter. The Custom setup options appear.

## Installation Prerequisites

```
Please enter the username to use sftp files off of this machine
Username [] nncentral
Please enter the password for the username
Password []
[ ] 1 - Check and Apply License [Default]
[ ] 2 - HTTP/HTTPS configuration
[ ] 3 - Fault Management configuration
[ ] 4 - Oracle Communications Session Delivery Manager cluster management
[X] 5 - Route Manager Central configuration
[ ] 6 - SAML Single sign on configuration
[ ] 7 - Mail Server configuration
[ ] 8 - Trunk Manager configuration
[ ] 9 - Quit setup
Please select an option [5]
```

### Removing Members from Cluster

There are two reasons why you would remove all members from a cluster. Either you are eliminating the cluster or you want to retain the cluster but remove a member. Both of these require you remove all members from the cluster. If you are eliminating the cluster, you are done. If you are removing a member, you need to re-add the members you want to retain to the cluster.

To remove members from the cluster:

1. Enter 4 and press Enter to choose Oracle Communications Session Delivery Manager cluster management. You are prompted about continuing.
2. Enter Y and press Enter to continue. The cluster management options appear.
3. Press Enter to retain the default value. You are prompted about continuing.
4. Enter Y and press Enter to continue. The add and remove members options appear.

```
Do you want to continue Yes/No?Y
Host name          | DB   | MOM   | Web Worker
                  | Port | Port  | Port
172.30.1.185      | 9000 | 61616 | 8009

===== Remote members =====
172.1.30.185      | 9000 | 61616 | 8009
172.30.80.19      | 9000 | 61616 | 8009
172.30.80.9       | 9000 | 61616 | 8009

Use the following options to add or remove members from cluster.
[ ] 1 - Add a new member
[ ] 2 - Remove all remote members
[ ] 3 - Apply new cluster configuration
[X] 4 - Cancel out and do not apply changes [Default]
```

```
Please select an option [4] []
```

5. Enter 2 to choose Remove all remote members and press Enter. You are prompted about continuing.
6. Enter Y to continue and press Enter. You are prompted that the operation removes all remote members from the edition configuration session. By default, the Cancel out of clear operation option is selected.

```
Do you want to continue Yes/No?Y
```

```
This operation will remove all remote members from the edition configuration session.
[ ] 1 - Proceed with removing all remote members
[X] 2 - Cancel out of clear operation [Default]
```

```
Please select an option [2] 1
```

7. Enter 1 to choose Proceed with removing all remote members. You are prompted about continuing.

8. Enter Y and press Enter to continue. All remote nodes are removed and only the host you are on which you are running Oracle Communications Session Delivery Manager is visible. The cluster management options also appear.

```
Do you want to continue Yes/No?Y
Host name          | DB    | MOM   | Web Worker
                  | Port  | Port  | Port
172.30.1.185      | 9000  | 61616 | 8009

Use the following options to add or remove members from cluster.
[ ] 1 - Add a new member
[ ] 2 - Remove all remote members
[ ] 3 - Apply new cluster configuration
[X] 4 - Cancel out and do not apply changes [Default]
```

Please select an option [4]

9. Enter 3 to apply the new cluster configuration to apply your changes. You are prompted about continuing.
10. Enter Y and press Enter to continue.

### Run Current Server as Standalone

You can configure the current server as a standalone to remove it from a cluster. All other members of the cluster are removed as well. You need to re-add any members you want to retain in the cluster.

1. Enter 2 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter to continue. The cluster member list appears with a warning that the server is part of a cluster and configuring it as a standalone removes it from the cluster. (All other members are removed as well and need to be re-added to the cluster if you want to retain them.)
3. Press Enter to continue configuring the server as a standalone. You are prompted about continuing.
4. Enter Y to continue and press Enter. All members of the cluster are removed and the current server is now considered a standalone.

```
Do you want to continue Yes/No?Y
Host name          | DB    | MOM   | Web Worker
                  | Port  | Port  | Port
localhost         | 9000  | 61616 | 8009

Please choose to quit cluster management or apply new configuration
[X] 1 - Configure and manage members in cluster [Default]
[ ] 2 - Run current host as a standalone
[ ] 3 - Quit out of cluster configuration
```

Please select an option [1]

5. Press Enter to configure and manage members in cluster if you want to retain the other members. You need to re-add them to recreate the cluster. Or enter 3 and press Enter to quit the cluster configuration.
6. Enter Y to continue and press Enter.

### Route Management Central

If you are licensed for the Route Manager application, you can access the Route Management Central configuration setup option. If you are not licensed for Route Manager, this setup option will not be visible.

1. Enter 7 and press Enter. You are prompted about continuing.
2. Enter Y and press Enter to continue. You are prompted for the maximum number of route set backups.

## Installation Prerequisites

---

Do you want to continue Yes/No?

=====

Route Manager Central configuration  
Configure Route Manager Central properties

Configure number of route set backups per route set/backup type combination  
Route Manager Central

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

3. Enter a value within range or press Enter to accept the default value. The Custom setup list of options appears. You can now configure SAML single sign-on.

### Configuring SAML Single Sign-On

If you are licensed for the Route Manager application, you can access the SAML single signon configuration setup option. If you are not licensed for Route Manager, this setup option will not be visible.

The Route Manager application supports login through an external server using SAML single sign-on. You enter a username and password used in the request to the external server for authentication. If using self-signed certificates, you can import them into the Route Manager certificates file (cacerts).

To configure SAML single sign-on:

1. Press Enter to accept the default value 6. You are prompted about continuing.

2. Enter Y and press Enter. You are prompted for the username,

```
SAML Single sign on configuration
Provides SAML Single sign on authentication.
```

```
SAML Single sign on
Configure SAML Single sign on
```

```
Please enter the username for basic authentication to SAML Responder
Username [] █
```

3. Enter the username for basic authentication and press Enter. You are prompted for the password.

```
Please enter the password for basic authentication to SAML Responder
Password [] █
```

4. Enter the password required for basic authentication and press Enter. You are prompted about the connection timeout.

```
Please enter the connection timeout to the SAML Responder
Connection timeout (seconds) (5-60) [5] █
```

5. Retain the default value 5. You are prompted about importing a certificate.

```
Would you like to import a certificate?
[ ] 1 - Yes
[X] 2 - No [Default]
```

```
Please select an option [2] █
```

If you do want to import a certificate, see the following section for details.

6. Press Enter to retain the default value No. You are done configuring SAML single sign-on.

7. Press Enter to quit setup. You are prompted about continuing.

8. Enter Y and press Enter to quit the setup program.

## Importing Certificates

To import certificates:

1. Enter 1 and press Enter to import certificates. You are prompted about continuing.

```
Please select an option [2] 1
```

```
[X] 1 - Yes
[ ] 2 - No [Default]
```

```
Do you want to continue Yes/No? █
```

2. Enter Y and press Enter. You are prompted for the import method.

```
Choose the import method
[X] 1 - File [Default]
[ ] 2 - HTTP mode
```

```
Please select an option [1] █
```

3. Press Enter to accept the default File. (If you choose the HTTP mode instead, you need to enter the same information.) You are prompted about continuing.

4. Enter Y and press Enter to continue. You are prompted for the alias name of the imported certificate.

```
Do you want to continue Yes/No?Y
```

```
Please enter the alias name for the imported certificate
Alias name [ ] █
```

5. Enter the alias name and press Enter. For example, acmep.csr. You are prompted for the certificate file.

```
Please enter the alias name for the imported certificate
Alias name [ ] acmep.csr
```

```
Please enter the certificate file
File [ ] █
```

6. Enter the name of the certificate file and press Enter. For example, apkt.cer. The loading process occurs and the certificate is added to the keystore using the alias. You are prompted about adding another.

7. Press Enter to accept the default value No. (Or Enter 1 to continue and repeat the steps for adding more.) You are prompted about continuing.

8. Enter Y to continue and press Enter.

## Installing Other Licensed Applications

If you hold a license for other Oracle Communications Session Delivery Manager applications, you can use the Custom Installation procedure to install the application.

To install your licensed application:

At the following prompt, enter the number associated with the licensed application you are installing (for example, Trunk Manager), and press Enter.

```
=====
[ ] 1 - Check and Apply License [Default]
[ ] 2 - OC SDM global identifier configuration
[ ] 3 - HTTP/HTTPS configuration
[ ] 4 - Fault Management configuration
[ ] 5 - Mail Server configuration
[ ] 6 - OC SDM cluster management
[ ] 7 - Route Manager Central configuration
[ ] 8 - SAML Single sign on configuration
[X] 9 - Trunk Manager configuration
```

## Installation Prerequisites

---

```
[ ] 10 - SBI TLS configuration
[ ] 11 - Quit setup
Please select an option [1] 1
=====
```

Follow the on-screen prompts to install the Oracle Communications Session Delivery Manager licensed application. For more information about your licensed application, see the respective Guide. For Trunk Manager installation procedures, see the SIP Trunk Xpress for Service Providers Guide.

## Exiting Setup

You can quit the setup utility after completing the custom installation procedure.

To exit the setup utility:

1. Enter 11 and press Enter to quit setup.

```
=====
[ ] 1 - Check and Apply License [Default]
[ ] 2 - OC SDM global identifier configuration
[ ] 3 - HTTP/HTTPS configuration
[ ] 4 - Fault Management configuration
[ ] 5 - Mail Server configuration
[ ] 6 - OC SDM cluster management
[ ] 7 - Route Manager Central configuration
[ ] 8 - SAML Single sign on configuration
[ ] 9 - Trunk Manager configuration
[ ] 10 - SBI TLS configuration
[X] 11 - Quit setup
Please select an option [1] 1
=====
```

2. Enter Y and press Enter to quit the setup program.

```
=====
Do you want to continue Yes/No? y
=====
```

## Starting the NNC Server

---

Before starting the Oracle Communications Session Delivery Manager server, you must exit out of root. This is necessary in order for the database to startup for the Report Manager.

To start the server:

1. Exit out of root.
2. Change to the bin directory. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Execute the startnnc.sh script.

```
./startnnc.sh
```

## Checking Running Processes

After you run startnnc.sh, 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.

Execute the report process status command on the server.

```
ps -eaf | grep AcmePacket
```

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



- Several httpd processes
- Three Java processes
- On some systems, you may see a fourth java process run from sudo. This is normal.

Below is an example of the system output:

```
nncentra 2494 2448 0 12:07:57 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
nncentra 2504 2448 0 12:09:57 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
root 2437 1 0 11:52:49 syscon 1:36 /apps/AcmePacket/NNC74/jre/bin/amd64/
java -Dlog4j.configuration=file:/apps/
root 2448 1 0 11:54:25 ? 0:00 httpd -d /apps/AcmePacket/NNC74/Apache/
httpserver -k start
root 2468 1 0 11:54:26 syscon 0:40 /apps/AcmePacket/NNC74/jre/bin/java -
Djava.util.logging.config.file=/apps/A
nncentra 2502 2448 0 12:09:56 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
nncentra 2542 2533 0 14:11:24 pts/2 0:00 grep Acme
nncentra 2501 2448 0 12:09:53 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
nncentra 2507 2448 0 12:12:11 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
root 2443 1 0 11:54:20 syscon 0:00 sudo -S /apps/AcmePacket/NNC74/jre/bin/
java -Dlog4j.configuration=file:/app
nncentra 2505 2448 0 12:10:00 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
nncentra 2500 2448 0 12:09:48 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
nncentra 2508 2448 0 12:12:11 ? 0:00 httpd -d /apps/AcmePacket/NNC74/
Apache/httpserver -k start
root 2445 2443 0 11:54:20 syscon 0:03 /apps/AcmePacket/NNC74/jre/bin/java
-Dlog4j.configuration=file:/apps/AcmePa
```

## Shutting down the Server

There are three procedures for shutting down Oracle Communications Session Delivery Manager depending upon your current configuration. Please refer to the applicable section below for the correct instructions.

### Standalone System

To shut down a standalone system:

1. Change directory to /NNC700/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

2. Execute the shutdownnnc.sh script.

```
./shutdownnnc.sh
```

### Cluster System for NNC 7.0

#### Manual Clean Cluster Shutdown


1. Log in to the other servers that are running replica databases.
2. Run the shutdownnnc.sh script.
3. Log in to the server running the master database.
4. Run the shutdownnnc.sh script.

## Installation Prerequisites

---

### Determine the Master Node for SDM 7.0 Clusters

1. Log in to the Oracle Communications Session Delivery Manager GUI client.

 **Note:** All cluster nodes must be up and running.

2. Access the Health Monitor to identify the server with the master database.
3. Identify the master database in one of two ways:
  - In the Heartbeat console, the server that is running the master database has (master) next to the IP address.
  - Run `grep "Role = master, IPAddress =" /opt/AcmePacket/<NNC directory>/logs/DbService.log`.

```
Msg:[Replicated Database environment initialization complete. Role =
master, IPAddress = 172.30.80.19]
```


### Cluster System for NNC 7.1+

To perform a cluster shutdown on Oracle Communications Session Delivery Manager 7.1+:

1. Change directory to /NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

2. Execute the `shutdownnnc.sh` script. The script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster.

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

```
[root@nms-vm12 bin]# ./shutdownnnc.sh
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)?Y
Shutting down cluster.....
```

3. Enter Y to continue and press Enter to shut down the cluster.

## Configuring the Acme Packet SBC for Session Delivery Manager Interaction

---

This section provides an example of how to configure the trap receiver and SNMP community in the Acme Packet SBC to point to the Oracle Communications Session Delivery Manager server. You need to configure these objects to enable Oracle Communications Session Delivery Manager to provide fault management (SNMP traps), performance management statistics, and inventory control (SNMP) for this specific SBC. If managing AP9000 SBCs, you need to create a virtual management interface to enable SOAP/XML (SNMP traps will also be sent to this virtual address).

You need to have Superuser privilege to configure your Acme Packet SBC through a terminal by way of a local or remote connection.

### Configuring the SNMP Interface

To configure the SNMP interface:

1. Connect to the Acme Packet SBC and login.
2. Enable Superuser mode. For example:

```
User Access Verification
Password: <User Mode password>
ORACLE> enable
Password: <Superuser Mode password>
ORACLE#
```

3. Execute the `configure terminal` command.

```
ORACLE# configure terminal
```

- Execute the system command.

```
ORACLE(configure)# system
```

- Execute the trap-receiver command.

```
ORACLE(system)# trap-receiver
```

- Enter the following information:

- ip-address <Oracle Communications Session Delivery Manager server IP address>
- filter-level <value>
- community-name <value>

For example:

```
ORACLE(trap-receiver)# ip-address 10.0.0.1
ORACLE(trap-receiver)# filter-level all
ORACLE(trap-receiver)# community-name acme
```

- Create a trap receiver for each Oracle Communications Session Delivery Manager server.

- Enter done. For example:

```
ORACLE(trap-receiver)# done
```

- Enter exit to return to the system level.

```
ORACLE(trap-receiver)# exit
```

- Execute the snmp-community command.

```
ORACLE(system)# snmp-community
```

- Enter the following information:

- ip-address <Oracle Communications Session Delivery Manager server IP address> or a list of IP addresses.  
For the Acme Packet 9000, ip-addresses add
- community-name <value>
- access-node <value> (leave at its default value)

For example:

```
ORACLE(snmp-community)# ip-address 10.0.0.1
ORACLE(snmp-community)# community-name acme
```

- Enter done. For example:

```
ORACLE(snmp-community)# done
```

- Enter exit to return to the system level.

```
ORACLE(snmp-community)# exit
```

- Execute the system-config command.

```
ORACLE(system)# system-config
```

- 

- Enter the following information:

```
ORACLE(system-config)# snmp-enabled enabled
```

- Enter done. For example:

```
ORACLE(system-config)# done
```

- Verify the information.

- Execute the save-config command (for Acme Packet 9000, use the save config command).

```
ORACLE(snmp-community)# save-config
```

- Execute the activate-config command to ensure SNMP is enabled (for Acme Packet 9000, use the activate command).

```
ORACLE# activate-config
```

## Installation Prerequisites

---

21. Enter the reboot command for AP4000 SBC (no need to reboot Acme Packet 9000).

```
ORACLE (snmp-community) # reboot
```

After the Acme Packet SBC system restarts, execute the show running-config command. The output should contain a trap receiver and SNMP community objects with the information you just configured.

## Starting the Oracle Communications Session Delivery ManagerClient and Connecting to the Server

---

Follow the instructions in this section to start the Oracle Communications Session Delivery Manager client and log in to the server.

If logging into Oracle Communications Session Delivery Manager when third-party X.509 certificates are used for HTTPS access, specify the hostname in DNS name format. Otherwise, the HTTPS you will have to click through security warnings about hostname mismatch between common name in the certificate and the IP address specified in the JNLP.



**Note:** You might experience difficulty connecting to Oracle Communications Session Delivery Manager because of your network's proxy support. If you have trouble connecting, check the proxy settings for both your browser. See *Verifying the Client System Settings* for more information.

## Verifying the Client System Settings

You should verify the client system has the required settings to connect to the Oracle Communications Session Delivery Manager server. You need to have the Oracle Communications Session Delivery Manager files from the distribution media at hand while verifying the client settings.

### Verifying the Internet Explorer Browser Settings

If using Internet Explorer as your browser, you need to verify the following settings.

1. Open the Internet Explorer browser.
2. Choose the Tools menu and click Internet options.
3. Choose the Security tab.
4. Choose the Local intranet option and click Custom Level.
5. Enable the following options (if not already enabled) then click OK.
  - Run ActiveX controls and plug-ins under ActiveX controls and plug-ins
  - Active Scripting and Scripting of Java applets under Scripting
6. Choose the Internet option on the Security tab and click Custom Level. (This step is required if the client system accesses the Oracle Communications Session Delivery Manager server via the Internet.)
7. Enable the following options (if not already enabled,) then click OK.
  - Run ActiveX controls and plug-ins under ActiveX controls and plug-ins
  - Active Scripting and Scripting of Java applets under Scripting

If you are running Internet Explorer 8, follow steps 8-12. If not, proceed to the final step.
8. Choose the Trusted Sites option on the Security tab and click Custom Level.
9. Enable the following options (if not already enabled,) then click OK.
  - Automatic prompting for file downloads under Downloads
10. Choose the Trusted Sites option on the Security tab and click the Sites button.
11. Add this website to the zone— Enter the Oracle Communications Session Delivery Manager server address in this field.
12. Click Add and then click Close.
13. Click OK on the Internet options window to close it.

### Disabling Proxy Server (Optional)

Follow these steps if your client system is configured as a proxy server and you do not want to use it for connecting with the Oracle Communications Session Delivery Manager server.

1. Open the Internet Explorer browser.
2. Choose the Tools menu and click Internet options.
3. Click the Connections tab on the Internet options screen.
4. Click LAN Settings and then click Advanced.
5. Enter the Oracle Communications Session Delivery Manager server IP address in the Exceptions panel.
6. Click OK.
7. Click OK on the Internet options window to close it.

### Starting the Oracle Communications Session Delivery Manager Client

You can start the Oracle Communications Session Delivery Manager client by using either the HTTP or HTTPS login:

```
http://<Oracle Communications Session Delivery Manager server IP address>:8080
https://<Oracle Communications Session Delivery Manager server IP address>:
8443 (self-signed certificates)
https://<domain name>:8443 (third-party X.509 certificates)
```



**Note:** If using third-party X.509 certificates, use the DNS name of the host such as `nncserver.acmepacket.com` instead of the IP address. Then it matches the common name in the certificate.



---

# Migrating Data to the Oracle Communications Session Delivery Manager

## Upgrading to Oracle Communications Session Delivery Manager 7.4


---

You can migrate data from older versions of Oracle Communications Session Delivery Manager to Oracle Communications Session Delivery Manager 7.4+ using the instructions below. The data migration tool will automatically detect older versions of Oracle Communications Session Delivery Manager during setup and prompt you with the option of migrating data.

### Requirements

The requirements for migrating data from an older version of Oracle Communications Session Delivery Manager include:

- Oracle Communications Session Delivery Manager 7.3+ installed on a Linux 6.2 machine prior to migration

 **Note:** You must follow a different upgrade path for earlier versions of Linux or SDM. See the *Upgrade SDM Across Platforms* section of this chapter for more information.

### Before You Migrate Data

Before you migrate data to a newer version of Oracle Communications Session Delivery Manager, you must delete or rename certain duplicate objects. Repeat steps until there are no longer duplicated objects in the listed areas.

#### Deleting Duplicate Devices

To delete duplicate devices from the Device column:

1. Expand the Device Manager > Devices.
2. Select the duplicate device and click Delete.

#### Renaming Duplicate Device Groups

To rename duplicate device groups:

1. Expand the Device Manager > Device group.
2. Select the duplicate device group and click Rename.

### Deleting Duplicate Users

To delete duplicate users:

1. Expand the Security Manager > User management > Users.
2. Select the duplicate user and click Delete.

### Deleting Duplicate User Groups

To delete duplicate user groups:

1. Expand the Security Manager > User management > Groups.
2. Select the duplicate user group and click Delete.

### Deleting Duplicate Work Orders

To delete duplicate work orders:

1. Expand the Device Manager > Software upgrade > Work order administration.
2. Select the duplicate work order and click Delete.

### Deleting Duplicate Global Work Orders

To delete duplicate global work orders:

1. Expand the Configuration Manager > Global parameters.
2. Click the Admin tab.
3. Select the duplicate work order and click Delete.

### Shutting Down NNC

Before you migrate data, you must make sure that Oracle Communications Session Delivery Manager is not running and execute the `setup.sh` script to configure the Oracle Communications Session Delivery Manager database and environment.

See Shutting down the Oracle Communications Session Delivery Manager Server for more information.

### Running `setup.sh`

To run `setup`:

1. Obtain the appropriate `tar.gz` file from the Oracle customer portal.
2. FTP the `tar.gz` file to your system. Place the file in the `opt/AcmePacket` directory where you have previously installed Oracle Communications Session Delivery Manager software.
3. Unzip the `*.tar.gz` file.

```
gunzip <filename>.tar.gz
```

4. Extract the files using one of the following command:

```
tar -xvf <filename>.tar
```

5. Change directory to `NNC74/bin`. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

6. Run the `setup.sh` script.

```
./setup.sh
```

The migration tool detects any previous versions of Oracle Communications Session Delivery Manager and prompts you based on whether the existing installation is a standalone or clustered system.

You can apply the Oracle Communications Session Delivery Manager license and complete the Oracle Communications Session Delivery Manager installation in standalone or cluster mode.

If you try to migrate data without running `setup` first, the following message appears.



Starting Migration Application 2011-05-25 14:11:27,086

Please run Oracle Communications Session Delivery Manager setup first. 2011-05-25 14:11:52,377

### Migrate Data from Older Versions of Net-Net Central

Ensure you first run setup.sh and have shutdown Route Manager Central before migrating data. Route Manager Central data files must be located on the same system as the Oracle Communications Session Delivery Manager installation.

#### Standalone System

To migrate data on a standalone 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 the a key anytime during the process will abort the current migration. You will not be able to launch the target version of Oracle Communications Session Delivery Manager until setup is re-run and database migration is performed.

```
Database migration beginning.
To abort and rollback database migration, press <a> then <enter> at any time
```

The database migration starts and progress information displays on the screen.

```
backing up existing database....done
migrating database...done
creating migrated master database archive...done
Database migration is now complete.
Press <enter> to continue with setup
```

3. Press enter to continue with Oracle Communications Session Delivery Manager Setup.

#### Clustered Systems Master Node

To migrate data on a master node:

1. Enter 1 to migrate 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>.
```

## Migrating Data to the Oracle Communications Session Delivery Manager

```
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. 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
Database migration beginning.
To abort and rollback database migration, press <a> then <enter> at any time
backing up existing database....done
migrating database...done
creating migrated master database archive...done
```

3. Enter 1 to copy the migrated 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 nodesz
[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
```

4. Enter Yes to continue.

```
[X] 1 - Copy the migrated database archive to other cluster nodes
[Default]
[ ] 2 - Do not copy the migrated database archive
Do you want to continue Yes/No? Yes
```

5. 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, upon successful migration you will see:

```
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
```

### Clustered Systems Replicated Node

To migrate data on a replicated node:

 **Note:** Setup must be performed on each replica member of the cluster.

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
```

Setup will proceed to the standard installation procedure.

You can now run startnnc.sh on cluster nodes.

## Upgrade SDM Across Platforms

You can migrate data from SDM while upgrading the server platform, using the instructions below.


### Requirements

The requirements for migrating data from an older version of Oracle Communications Session Delivery Manager include:

- Oracle Communications Session Delivery Manager 7.3M4 installed on a Linux 5.5 machine

## Migrating Data to the Oracle Communications Session Delivery Manager

- External location for data backup
- Supported Linux 6.3/6.4/6.5 distribution
- SDM 7.3M4 for Linux 6.3/6.4/6.5 installation image
- SDM 7.4 for Linux 6.3/6.4/6.5 installation image

 **Note:** You must follow a different upgrade path for newer versions of Linux or SDM. See the *Installing Session Delivery Manager* chapter for more information on installing and upgrading current versions of SDM.

### Before You Start


Before you begin to migrate data and upgrade server components, you must identify the SDM version and Linux release you are currently running. The following steps point to the relevant upgrade and migration instructions for each set up.

SDM Deployment	Sections to Follow
SDM 7.3M4 on Linux 5.5	<ol style="list-style-type: none"><li>1. Upgrade the Server Platform</li><li>2. Migrate Data Across Platforms</li><li>3. Upgrade to SDM 7.4</li></ol>
SDM 7.3M4 on Linux 6.3/6.4/6.5	<ol style="list-style-type: none"><li>1. Migrate Data Across Platforms</li><li>2. Upgrade to SDM 7.4</li></ol>

### Upgrade the Server Platform


This process allows you to backup your database information and upgrade the SDM server OS to a supported version of Linux.


1. Log into the SDM 7.3M4 server that you wish to upgrade.
2. Navigate to **Tools > Health Monitor** to identify which member of the SDM cluster is the master.

 **Note:** Only a single server will appear for standalone deployments.

3. Log into the host SDM 7.3M4 Server.
4. Enter `shutdownnnc.sh` and press `<enter>`.

```
shutdownnnc.sh
```

 **Note:** Verify that all processes on the SDM servers are down.

5. Perform a cold backup of 7.3M4 on the master host machine, selecting all options.  
 **Note:** Store the backup files in a remote location.
6. Upgrade the server OS from Linux 5.5 to 6.3/6.4/6.5 according to the instructions provided with your supported distribution.
7. Remove any files from the previous SDM 7.3M4 installation, if not taken care of the system in step 6.

### Migrate Data Across Platforms

This process allows you to import your database information to SDM running on a newer version of Linux.

1. FTP the cold backup data from a remote location to the upgraded server.
2. Restore the cold backup.
3. Run `startnnc.sh` and press `<enter>`.

```
startnnc.sh
```

4. Verify that all data is populated as expected.

5. Run `shutdownnnc.sh` and press `<enter>`.

```
shutdownnnc.sh
```



**Note:** Verify that all processes on the SDM servers are down.

### Upgrade to SDM 7.4

This process describes the 7.4 upgrade scenario for a system running 7.3M4 on Linux 6.3/6.4/6.5.

1. Install SDM 7.4 per the *Installing Session Delivery Manager* chapter to initiate data migration.
2. Run `startnnc.sh` to ensure that all data is migrated.

```
startnnc.sh
```

### Cluster Setup and Migration

This process allows you to set up and deploy clustered SDM environments with the latest software version.

1. FTP the 7.3M4 cold backup data from the previous section to the upgraded server.
2. Restore the cold backup.
3. Run `shutdownnnc.sh` to stop each server node.

```
shutdownnnc.sh
```



**Note:** Verify that all process on the SDM servers are down.

4. Install SDM 7.4 on the master server.
5. Run a cold backup on the master machine with all options selected.



**Note:** Store the backup files in a remote location.

6. Uninstall previous versions of SDM and install 7.4 on each replica node.
7. FTP the cold backup data from a remote location to each replica node.
8. Restore the cold backup.
9. Run `startnnc.sh` and press `<enter>`.

```
startnnc.sh
```

## EMS 6.x to Oracle Communications Session Delivery Manager 7.3

---

The instructions below follow data migration from Net-Net EMS 6.x or Route Manager 1.x to Oracle Communications Session Delivery Manager 7.3, and earlier versions of Oracle Communications Session Delivery Manager to Oracle Communications Session Delivery Manager 7.3.

You can migrate the following information from EMS 6.x to Oracle Communications Session Delivery Manager 7.3:

- User profile
- Alarms and events
- Device list and SBC node information: IP addresses and passwords.
- Banner text
- Audit trail logs



**Note:** Configuration data is not migrated.

### Migration Process

Data migration from Net-Net EMS 6.x to Oracle Communications Session Delivery Manager 7.3 is launched and handled by the data migration tool, ensuring data from fault management, user security, and devices is migrated.

The data migration tool retrieves data from the old databases, saving it to different categories of intermediate XML files that are compliant with the Berkeley DB XML (dbxml) files on the embedded Oracle Communications Session Delivery Manager database. When you run Oracle Communications Session Delivery Manager, the migrated data is available.

### Requirements

The requirements for migrating data from Net-Net EMS 6.x include:

- Net-Net EMS 6.x database running
- Host name of the MySQL server
- MySQL port number
- Database user account with permissions allowing execution of SQL query
- User name and password of database user account
- Database name of Net-Net EMS data stored

### Before You Migrate Data

Before you migrate data, you must make sure that Oracle Communications Session Delivery Manager is not running and execute the `setup.sh` script to configure the Oracle Communications Session Delivery Manager database and environment.

See [Shutting down the Oracle Communications Session Delivery Manager Server](#) for more information.

To run setup:

1. Obtain the appropriate `tar.gz` file from the Oracle customer portal.
2. FTP the `tar.gz` file to your system. Place the file in the `opt/AcmePacket` directory where you have previously installed Oracle Communications Session Delivery Manager software.
3. Unzip the `*.tar.gz` file.

```
gunzip <filename>.tar.gz
```

4. Extract the files using one of the following command:

```
tar -xvf <filename>.tar
```

5. Change directory to `NNC74/bin`. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

6. Run the `setup.sh` script.

```
./setup.sh
```

The migration tool detects any previous versions of Oracle Communications Session Delivery Manager and prompts you based on whether the existing installation is a standalone or clustered system.

You can apply the Oracle Communications Session Delivery Manager license and complete the Oracle Communications Session Delivery Manager installation in standalone or cluster mode.

If you try to migrate data without running setup first, the following message appears.

```
Starting Migration Application 2011-05-25 14:11:27,086
Please run Oracle Communications Session Delivery Manager setup
first. 2011-05-25 14:11:52,377
```

## Migrating Data from EMS 6.x to Oracle Communications Session Delivery Manager 7.3

To migrate data from Net-Net EMS 6.x:

Ensure you have run `setup.sh` first and have shutdown Oracle Communications Session Delivery Manager before you migrate data.

The default user groups Admin, Monitor, and Provisioner are not migrated. Oracle Communications Session Delivery Manager creates those default groups with different names. Users are migrated but their passwords are reset to their usernames. When users log in for the first time, they need to change their passwords.

1. Log in as root.
2. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Run the `dataMigration.sh` script to start the migration.

```
./dataMigration.sh
```

The migration options appear.

```
Migration Options:
```

```
1 EMS 6.x      : Migrating data from EMS 6.x to NNC 7.x
2 RMC 1.x     : Migrating data from RMC 1.x to NNC 7.x
3 Quit.
Select [1]
```

4. Press Enter to accept the default and migrate data from Net-Net EMS 6.x. You are prompted for the hostname or IP address.

```
Hostname or IP (required):
```

5. Enter the DNS name of the host or the IP address and press Enter. You are prompted for the port number.

```
Port [3306]:
```

6. Press Enter to accept the default value 3306 or enter a new port number and press Enter. You are prompted for the user name.

```
User [root]:
```

7. Press Enter to accept the default value or enter your username. You are prompted for the password.

```
Password:
```

8. Enter the password and press Enter. The data migration starts and the status appears on the screen.

```
Connected to database 2011-05-24 17:49:19,602
Migrating alarms data ... 2011-05-24 17:49:19,603
Migrating events data ... 2011-05-24 17:49:19,734
Migrating device groups data ... 2011-05-24 17:49:19,801
Migrating fault data ... 2011-05-24 17:49:19,907
Migrating ems details data ... 2011-05-24 17:49:19,934
Migrating device details data ... 2011-05-24 17:49:20,103
Migrating user security data ... 2011-05-24 17:49:20,142
Migrating audit trail logging data ... 2011-05-24 17:49:21,843
Start to load data into database 2011-05-24 17:49:22,104
Loading: alarms.xml into database ... 2011-05-24 17:49:22,530
Loaded: alarms.xml into database successfully. 2011-05-24 17:49:22,596
Loading: events.xml into database ... 2011-05-24 17:49:22,596
Loaded: events.xml into database successfully. 2011-05-24 17:49:22,640
Loading: AuditTrail.xml into database ... 2011-05-24 17:49:22,640
Loaded: AuditTrail.xml into database successfully. 2011-05-24 17:49:22,695
Loading: EMSDetails.xml into database ... 2011-05-24 17:49:22,949
Loaded: EMSDetails.xml into database successfully. 2011-05-24 17:49:23,031
Loading: Fault.xml into database ... 2011-05-24 17:49:23,032
Loaded: Fault.xml into database successfully. 2011-05-24 17:49:23,053
Loading: DeviceGroup.xml into database ... 2011-05-24 17:49:23,054
```

## Migrating Data to the Oracle Communications Session Delivery Manager

```
Loaded: DeviceGroup.xml into database successfully. 2011-05-24 17:49:23,093
Loading: DeviceDetails.xml into database ... 2011-05-24 17:49:23,093
Loaded: DeviceDetails.xml into database successfully. 2011-05-24
17:49:23,128
Loading: UserSecurity.xml into database ... 2011-05-24 17:49:23,128
Loaded: UserSecurity.xml into database successfully. 2011-05-24 17:49:23,227
Loaded data into database successfully 2011-05-24 17:49:23,227
Disconnected from database 2011-05-24 17:49:23,229
Completed data migration successfully! 2011-05-24 17:49:23,230
[nncentral@cosmo bin]#
```


Any new rules and attributes required by Oracle Communications Session Delivery Manager are added during the migration process.

## Net-Net EMS 6.X to Oracle Communications Session Delivery Manager 7.3 Database Migration Information

### Running Database Migration Again

You cannot run database migration a second time without re-initializing the Oracle Communications Session Delivery Manager database first. Reinitializing the database permanently clears all the data it contains.

To reinitialize a database:

 **Note:** This section only applies to migration from EMS 6.x to NNC7.x. Following these steps for Oracle Communications Session Delivery Manager 7.x to NNC7.3 migrations may result in data loss.

1. Log in to the Oracle Communications Session Delivery Manager server as root user.
2. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Enter the following command to reinitialize the database:

```
./reinitialize.sh
```

### Reinitialize Database with Data

```
./reinitialize.sh
Reinitialize options
[ ] 1 - Reintialize: This will clear all databases
[X] 2-Quit : Exit Reintialize
Select an option [2] 1
Warning : This will delete all the content in database. Do you want to
continue Yes/No ?yes
Deleting file ../../db/local/data/alarms.dbxml ...
Deleting file ../../db/local/data/AuditTrail.dbxml ...
Deleting file ../../db/local/data/___db.001 ...
Deleting file ../../db/local/data/___db.002 ...
Deleting file ../../db/local/data/___db.003 ...
Deleting file ../../db/local/data/___db.004 ...
Deleting file ../../db/local/data/___db.005 ...
Deleting file ../../db/local/data/___db.006 ...
Deleting file ../../db/local/data/events.dbxml ...
Deleting file ../../db/local/data/log.00000000001 ...
Deleting file ../../db/replicated/data/___db.001 ...
Deleting file ../../db/replicated/data/___db.002 ...
Deleting file ../../db/replicated/data/___db.003 ...
Deleting file ../../db/replicated/data/___db.004 ...
Deleting file ../../db/replicated/data/___db.005 ...
Deleting file ../../db/replicated/data/___db.006 ...
Deleting file ../../db/replicated/data/DeviceDetails.dbxml ...
Deleting file ../../db/replicated/data/DeviceGroup.dbxml ...
```



```
Deleting file ../../db/replicated/data/EMSDetails.dbxml ...
Deleting file ../../db/replicated/data/Fault.dbxml ...
Deleting file ../../db/replicated/data/log.0000000001 ...
Deleting file ../../db/replicated/data/UserSecurity.dbxml ...
Deleting file ../../db/local/migrationdb/alarms.xml ...
Deleting file ../../db/local/migrationdb/AuditTrail.xml ...
Deleting file ../../db/local/migrationdb/events.xml ...
Deleting file ../../db/replicated/migrationdb/DeviceDetails.xml ...
Deleting file ../../db/replicated/migrationdb/DeviceGroup.xml ...
Deleting file ../../db/replicated/migrationdb/EMSDetails.xml ...
Deleting file ../../db/replicated/migrationdb/Fault.xml ...
Deleting file ../../db/replicated/migrationdb/UserSecurity.xml ...
```

### Reinitialize Database without Data

```
./reinitialize.sh
Reinitialize options
[ ] 1 - Reintialize: This will clear all databases
[X] 2-Quit : Exit Reintialize
Select an option [2] 1
Warning : This will delete all the content in database. Do you want to
continue Yes/No ?yes
```

## Data Migration Logging

Information about the data migration flow is captured in the Migration.log file located in the /AcmePacket/NNC74/logs directory.

The information includes:

- Net-Net EMS 6.x
  - MySQL database open/close connection
  - User management and security
  - Alerts
  - Events
  - Device Details
  - Device Groups
  - Audit trails
  - Fault
  - Banner
- Route Manager Central 1.x
  - Berkeley database XML open/close containers
  - Database connection
  - User management and security
  - Device Details
  - Device Groups
  - Audit trails
  - Route sets
  - Route Management System (RMS)

## Error Logging

Errors are logged as well as the data migration flow information. If errors in data migration occur, you need to reinitialize the database before you can retry the migration.

## Mapping Device Groups to User Groups

After the data migration occurs, the devices exist in the Oracle Communications Session Delivery Manager database but they might not be immediately visible in the Oracle Communications Session Delivery Manager GUI. You need to map device groups to user groups for security purposes. Until that mapping is created, users in the user groups will not be able to see any of the devices in the device group.

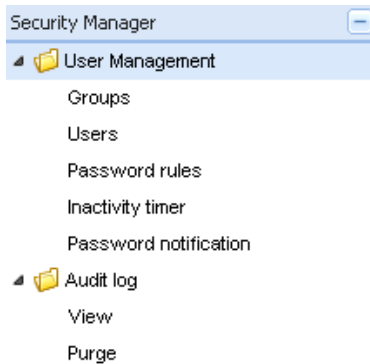
The Oracle Communications Session Delivery Manager administrator must decide which of the device groups can be seen and managed by which the default user groups that are created by default when Oracle Communications Session Delivery Manager is installed:

- administrators: Super user group privileged to perform all operations
- LIAdministrators: Privileged to perform most operations including Lawful Intercept (LI) configuration changes
- provisioners: Privileged to configure SBCs (if licensed for Element Manager) and save and apply the configuration with the exception of a LI configuration.
- monitors: Privileged to only view data, both configuration and other kinds of data.

Oracle recommends that all four of the default user groups have full visibility into all migrated device groups.

To map device groups to user groups:

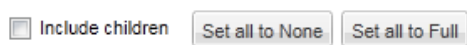
1. Log in to Oracle Communications Session Delivery Manager as admin.
2. Expand the Security slider in the Navigation bar.
3. Expand the User Management directory.



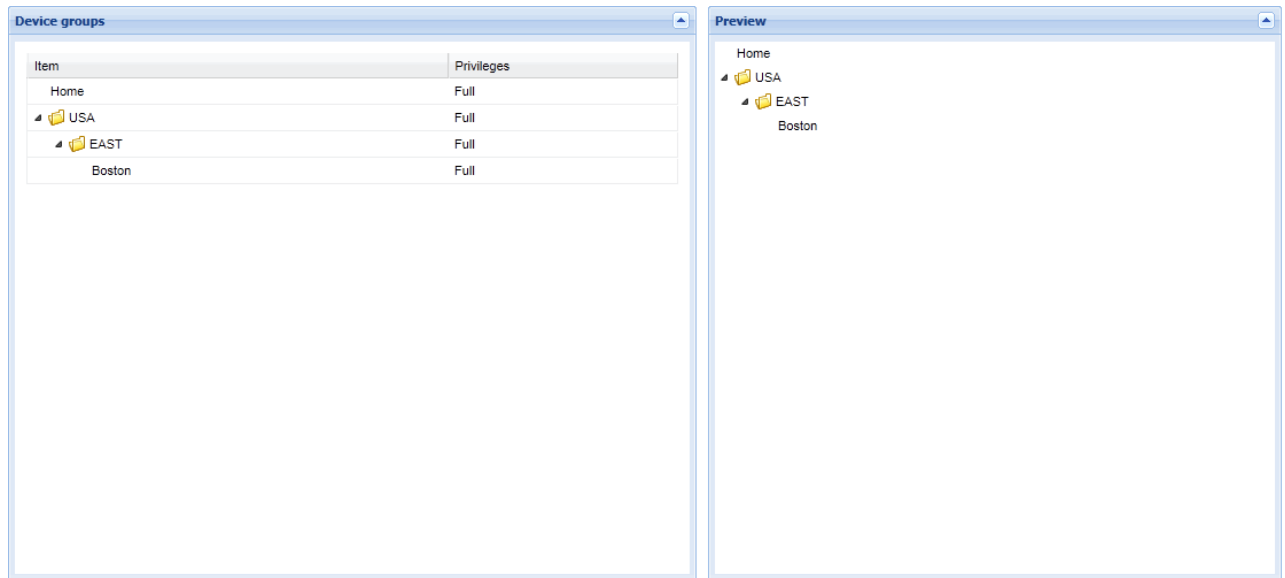
4. Click Groups in the Navigation bar. A table of user groups appears in the content body. The table displays all of the operations categories with the current privilege levels for each user group.
5. Click a user group name in the table and click Edit. For example, click LIAdministrators. The operations tabs appear.

Configuration	SBC system maintenance	Administrative operations	Fault management	Device group instances
Item				Privileges
▶ Configuration				Full

6. Click Device group instances. The Device group instances tab lets you assign privileges and preview the device group hierarchy based on the privileges selected. That hierarchy will be reflected on the Device Manager slider.
7. Click Set all to Full.



The permissions on all device groups is set to Full. The device groups appear in the Preview column.



8. Click Apply.
9. Repeat steps 4 through 7 to assign privileges to each user group.

## Migrating Route Manager Data

You can migrate the following information from the Route Management database.

- User profile
- Route Sets
- Device list and node information: IP addresses and passwords. Configuration data is not migrated.
- Banner text
- Audit trail logs

## Migration Process

Data migration from Route Manager 1.x to Oracle Communications Session Delivery Manager 7.3 is launched and handled by the data migration tool, ensuring data from fault management, user security, and devices is migrated.

The data migration tool retrieves data from the old databases, saving it to different categories of intermediate XML files that are compliant with the Berkeley DB XML (dbxml) files on the embedded Oracle Communications Session Delivery Manager database. When you run Oracle Communications Session Delivery Manager, the migrated data is available.

## Requirements

The requirements for migrating data from Route Manager 1.x include:

- Path to database entry folder. For example, on Linux:

```
opt/ACMEPacket/rmc/db
```

- Stopping Route Manage

## Before You Migrate Data

Before you migrate data, you must make sure that Route Manager Central and Oracle Communications Session Delivery Manager are not running and execute the `setup.sh` script to configure the Oracle Communications Session Delivery Manager database and environment.

To run setup:

## Migrating Data to the Oracle Communications Session Delivery Manager

---

1. Obtain the appropriate tar.gz file from the Oracle customer portal.
2. FTP the tar.gz file to your system. Place the file in the opt/AcmePacket directory where you have previously installed Oracle Communications Session Delivery Manager software.
3. Unzip the \*.tar.gz file.

```
gunzip <filename>.tar.gz
```

4. Extract the files using one of the following command:

```
tar -xvf <filename>.tar
```

5. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

6. Run the setup.sh script.

```
./setup.sh
```

The migration tool detects any previous versions of Oracle Communications Session Delivery Manager and prompts you based on whether the existing installation is a standalone or clustered system.

You can apply the Oracle Communications Session Delivery Manager license and complete the Oracle Communications Session Delivery Manager installation in standalone or cluster mode.

If you try to migrate data without running setup first, the following message appears.

```
Starting Migration Application 2011-05-25 14:11:27,086
Please run Oracle Communications Session Delivery Manager setup
first. 2011-05-25 14:11:52,377
```

## Migrating from Route Manager 1.x

To migrate data from Route Manager:

Ensure you have run setup.sh first and have shutdown Route Manager Central before you migrate data. The Route Manager Central data files need to be located on the same system as Oracle Communications Session Delivery Manager.

1. Log in as root.
2. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Run the dataMigration.sh script to start the migration.

```
./dataMigration.sh
```

The migration options appear.

```
Migration Options:
```

```
1 EMS 6.x      : Migrating data from EMS 6.x to NNC 7.x
2 RMC 1.x      : Migrating data from RMC 1.x to NNC 7.x
3 Quit.
Select [2]
```

4. Enter 2 and press Enter to migrate data from RMC 1.x. You are prompted for the path to the dbxml files.

```
Path to RMC dbxml files (required):
```

5. Enter the path to the files and press Enter.

```
/opt/ACMEPacket/rmc/db
```

The database migration starts and progress information displays on the screen.

```
Migrating ems details data ... 2011-05-26 14:49:11,155
Migrating device details data ... 2011-05-26 14:49:11,467
Migrating user security data ... 2011-05-26 14:49:12,264
Migrating audit trail logging data ... 2011-05-26 14:49:12,295
Start to load data into database 2011-05-26 14:49:13,052
Loading: AuditTrail.xml into database ... 2011-05-26 14:49:13,177
```

## Migrating Data to the Oracle Communications Session Delivery Manager

---

```
Loaded: AuditTrail.xml into database successfully. 2011-05-26 14:49:16,863
Loading: EMSDetails.xml into database ... 2011-05-26 14:49:17,332
Loaded: EMSDetails.xml into database successfully. 2011-05-26 14:49:18,316
Loading: DeviceDetails.xml into database ... 2011-05-26 14:49:18,316
Loaded: DeviceDetails.xml into database successfully. 2011-05-26
14:49:18,621
Loading: UserSecurity.xml into database ... 2011-05-26 14:49:18,621
Loaded: UserSecurity.xml into database successfully. 2011-05-26
14:49:18,941
Loading: rms.xml into database ... 2011-05-26 14:49:18,949
Loaded: rms.xml into database successfully. 2011-05-26 14:49:19,245
Loaded data into database successfully 2011-05-26 14:49:19,245
Completed data migration successfully! 2011-05-26 14:49:19,245
```



---

## Installing Oracle Communications Session Delivery Manager Patches

This section explains how to install Oracle Communications Session Delivery Manager software patches using the Oracle Communications Session Delivery Manager patch management tool. This process is applied for patches subsequent to Oracle Communications Session Delivery Manager software release version 7.4.

To install patches beyond Oracle Communications Session Delivery Manager 7.4, you need to obtain the appropriate patch tar.gz file for your environment from your Oracle representative. You also must have Oracle Communications Session Delivery Manager already installed and have run setup before. The patch management tool is distributed with the Oracle Communications Session Delivery Manager GA software release.

The patch management tool allows you to perform the following operations:

- List imported patches
- Import patches
- Apply a patch
- Remove patches

You FTP the patch tar.gz to a directory on your system. The location is not specified. Note the path for your own reference when the patch management tool prompts you for the file location. When directed, the patch management tool unzips and extracts the necessary files, and places them in the original Oracle Communications Session Delivery Manager installation directory, appending a /patches directory where the patch files will be located.

You can run the patch management tool while the Oracle Communications Session Delivery Manager server is running, but you will be restricted to the following options:

- List available patches on the system.
- Import the patches.

In order to apply or remove patches, the Oracle Communications Session Delivery Manager server must be shut down.

Patches are cumulative in that patch 5 contains patches 1-4 as well.

Once you have successfully applied a new patch with the patch management tool, you can verify the new Oracle Communications Session Delivery Manager software version by performing one of the following actions:

- Use the tool to list imported patches. The current version is marked with an asterisk.
- Once the server is started, Click Help > About in the Oracle Communications Session Delivery Manager GUI.

### Shutting Down Oracle Communications Session Delivery Manager Servers

---

You must shutdown the Oracle Communications Session Delivery Manager server in order to apply or remove patches. See Shutting down the Oracle Communications Session Delivery Manager Server for more information.

### Running the Patch Management Tool in a Cluster

---

In order to run the patch tool in a cluster, you must shutdown all nodes in a cluster, and apply the patch manually for each cluster. The recommended steps for this process are to:

1. Shutdown Oracle Communications Session Delivery Manager servers in the cluster.
2. Apply the patch to each Oracle Communications Session Delivery Manager host in the cluster.
3. Startup the Oracle Communications Session Delivery Manager servers in the cluster.

### Identifying the Master Node Patch Version in a Cluster

During the startup sequence, if a node in a cluster is not at the same patch version as the master node, the startup terminates and an error message is displayed.

```
System is at NNC74P1, Master is at NNC74P2. All hosts must be at same patch level. Terminating startup.
```

### Installing Oracle Communications Session Delivery Manager Patches

---

To run the patch management tool:

1. Log in to the Oracle Communications Session Delivery Manager server as root.
2. Navigate to the bin directory. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Run the patchManagement.sh script.

```
./patchManagement.sh
```

A Welcome message appears and initialization processes occur. Patch management checks that minimal system requirements are met and whether the system is running.

```
cd /opt/AcmePacket/NNC74/bin
[root@nncentral bin]# ./patchManagement.sh
=====
Welcome to Oracle Communications Session Delivery Manager Patch Management
application
Current Oracle Communications Session Delivery Manager Version: NNC74P1
OS : Linux : amd64 : 2.6.18-194.el5
=====
Please wait while application loads
Checking environment for patch management application.
Please wait ....
100%[=====]
Patch Management Menu
Please select from the following options:
[X] 1 - List Imported patches
[ ] 2 - Import patch
[ ] 3 - Apply patch
[ ] 4 - Remove all applied patches
```



```
[ ] 5 - Quit
Please select an option [1]
```

You must select an option to perform one of the following options:

4. List imported patches
5. Import patches
6. Apply a patch
7. Remove patches
8. Quit

The options are described below.

### Listing Imported Patches

To list the patches available on the system, select option 1 in the prompt.

The patch management tool checks the system for available patches. If the current-running software version is a patch, that version will have an asterisk [\*]beside it.

```
=====
LIST_IMPORTED_PATCH
This option will list all imported patches
(*) Current Patch Level
NNC74P1*
=====
```

### Importing Patches

To import patches, select option 2 in the prompt.

1. Patch file name [ ]—When prompted, enter the patch file name and its full directory path. For example:

```
/opt/NNC74P1Linux64bit.tar.gz
```

2. Hit Enter.

The patch management tool performs the following actions sequentially:

- Checks that the import directory and patch file specified by the user exists.
- Checks that the parent destination directory exists. If not, the parent directory, /patches, is created.
- Checks whether a patch directory with the same name already exists. If so, the tool displays a message indicating that this patch has already been imported. The tool backs out from this option, and the user can select another option.
- Extracts the patch version information from the tar.gz file.
- Checks that the patch version matches the current Oracle Communications Session Delivery Manager GA version. If a mismatch is detected, an error message is displayed indicating that the patch version is not applicable to the current GA version. The extracted file is removed and the import process is halted.
- If the version check is successful, the tool extracts the remaining contents of the patch.
- Checks each file's MD5 hash to ensure the files are valid. If a discrepancy is detected during this process, the patch is considered corrupted and is removed from the patches directory. An error message is displayed.

Below is the output for a successful patch import:

```
=====
IMPORT_PATCH
This option will import a user specified patch
Please specify the patch file to import with full path
Patch file name [ ] /opt/NNC74P1Linux64bit.tar.gz
Patch file name [/opt/NNC74P1Linux64bit.tar.gz]
100%[=====]
```

### Applying Patches

To apply patches, select option 3 in the prompt.

If you select option 3 to apply the patch, the patch tool checks to see if the Oracle Communications Session Delivery Manager server is running. You cannot apply the patch if the server is running.

```
=====
APPLY_PATCH
This option allows the end user to apply an imported patch
to the destination directory
Checking the server status....
Oracle Communications Session Delivery Manager server is running
The option can not be performed when server is running
```

If the server is shut down, the patch tool displays a list of available patches on the system, and prompts you to select a patch.

The system will ask if you wish to continue. If you select Yes, the patch management tool performs the following actions sequentially:

- If the selected patch version is the same as the current-running patch version, the tool stops. The tool will prompt you to select one of two options: go back to the main menu, or select another patch to apply.
- If the current-running software version is a patch, the system is rolled back to the GA software version first, and then proceed to the next step. If the current-running version is not a patch, it will proceed to the last step.
- Backs up the GA software version and files that the target patch will replace.
- Applies the targeted patch.

A success message is displayed once a patch is successfully applied.

```
(*) Current Patch Level
[ ] 1. NNC74P1 (*)
[ ] 2. NNC74P2
[ ] 3. NNC74P5
[X] 4. Quit
Please select an option [4] 2
[ ] 1. NNC74P1 (*)
[X] 2. NNC74P2
[ ] 3. NNC74P5
[ ] 4. Quit
Do you want to continue Yes/No?
Patch applied successfully!
```

### Removing All Applied Patches

To remove patches, select option 4 in the prompt.

If you select option 4 to uninstall all patches, the patch tool checks to see if the Oracle Communications Session Delivery Manager server is running. You cannot remove patches if the server is running. If the server is running, the system sends a warning message:

```
=====
ROLLBACK_TO_GA
This option allows the end user to remove the current installed patch
Oracle Communications Session Delivery Manager Server is running
The option can not be performed when server is running
```

If the server is not running, the patch management tool performs the following actions sequentially:

- If the current-running software version is a patch, the system is rolled back to the GA software version first. If the current-running version is not a patch, the tool completes the process.

The patch tool displays the following confirmation:

```
=====
ROLLBACK_TO_GA
```

```
This option allows the end user to remove the current installed patch
Do you want to rollback from the current version NNC74P1 to the GA release
[ ] 1 - Yes
[X] 2 - No [Default]
Please select an option [2] 1
[X] 1 - Yes
[ ] 2 - No [Default]
Do you want to continue Yes/No?y
Starts to rollback from NNC74P1 to GA release
Applied patch removed successfully
```

## Re-establishing User-Configured Setup Configurations

It is possible that applying a new patch modifies user-configured setup options. In the event that setup files are modified, the setup process attempts to reapply the last setup configurations. This process is comprised of three components:

**Pre-condition-Checks** to see if there is a version change for this session. If so, it checks to see if the current version modified any of the setup configuration files.

**User-required Inputs**-It is possible you will be asked to input information for external dependencies such as license file location.

**Post-process**-If required, performs internal processes for reapplying the original setup configuration. The screen output for this process is shown below:

If you decide not to run the auto-setup, it is possible that setup will not run properly. If you select No, you will receive a warning message.

```
Auto Setup pre-checking starts...
Current installed version: NNC74P1 Initial installed version: NNC74
Detect setup configuration file change!
Done pre-checking for Auto Setup
Auto Setup is needed
Do you want to continue Yes/No?
=====
Welcome to Auto Setup Application
Version : NNC74
OS : Linux : amd64 : 2.6.18-194.26.1.el5
=====
Please wait while application loads
WARNING!!!! This process will automatically apply the previous setup
Do you want to continue Yes/No?
Checking environment and setting permissions.
Please wait ....
100%[=====]
=====
System Physical Memory Diagnostics
Total System Physical Memory = 24098 MB
Total System Free Physical Memory = 1637 MB
=====
System Disk Space Diagnostics
Total System Disk Space = 144 GB
Free System Disk Space = 93 GB
WARNING: Disk space is insufficient for running this application.
The recommended total disk space that should be available is = 300 GB
=====
System Port Availability Diagnostics : Oracle Communications Session Delivery
Manager Required Ports
The following port is available [ 5000 ]
The following port is available [ 8080 ]
The following port is available [ 61616 ]
The following port is available [ 9000 ]
```

## Installing Oracle Communications Session Delivery Manager Patches

---

```
The following port is available [ 8443 ]
The following port is available [ 1099 ]
The following port is available [ 8009 ]
The following port is available [ 1098 ]
The following port is available [ 8005 ]
=====
Auto setup completed for CHECK_APPLY_LICENSE
=====
HTTP/HTTPS configuration
No previous setup information found for HTTP
Auto setup completed for HTTPS
=====
Fault Management configuration
Auto setup completed for TRANSITION_HIDE
=====
Oracle Communications Session Delivery Manager cluster management.
No previous setup information found for CLUSTER_MEMBERSHIP
No previous setup information found for ROUTE_MGMT_SFTP
=====
Route Manager Central configuration
No previous setup information found for ROUTE_MGMT
=====
SAML Single sign on configuration
SANE does not support AutoSetup! Manual setup is required for this
configuration
=====
Mail Server configuration
No previous setup information found for CONFIG_MAIL_SERVER
Exit Auto Setup Application
```

---

# Troubleshooting

---

## Missing Libraries

---

The SDM installation process runs a system package diagnostic against the operating system to alert you of any missing required libraries.

Issues relating to missing libraries can be resolved by identifying and installing the missing packages using the YUM provides and install commands. The following is an example of a missing required shared library notification during the installation process:

```
System Package Diagnostics
ERROR: Missing required shared library libXxf86vm.so.1
```

To identify and install missing system packages:

1. Enter `yum provides <missingLibrary>` to identify the missing system package.

```
# yum provides libXxf86vm.so.1
Loaded plugins: fastestmirror
Determining fastest mirrors
libXxf86vm-1.0.1-3.1.i386 : X.Org X11 libXx86vm runtime library
Repo      : centos510_x86_64
Matched from:
Other     : libXxf86vm.so.1
```

2. Enter `yum install <missingPackage>` to install the missing system package.

```
# yum install libXxf86vm
```

 **Note:**

Running `setup.sh` allows the system package diagnostic to verify that the missing libraries are installed and accessible to SDM.

