Oracle® Communications
Report Manager User Guide

Release 8.1

December 2018

ORACLE®

Oracle Communications Report Manager User Guide, Release 8.1

Contents

ORACLE

5 Reset Passwords for Oracle and BI Publisher Database Users

About This Guide

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

Oracle Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Related Documentation

Table   Oracle Communications Product Plug-in Documentation Library

Document Name	Description
Session Element Manager User Guide	Provides information for managing and optimizing network infrastructure elements and their functions with comprehensive tools and applications used to provision fault, configuration, accounting, performance, and security (FCAPS) support for managed network functions and their associated devices in Oracle Communications Session Delivery Manager (SDM).
Report Manager User Guide	Provides information about configuring Report Manager to interoperate with Oracle BI Publisher as well as creating reports on Session Delivery product network devices.
Report Manager Installation Guide	Provides information for installing Oracle Communications Report Manager product as an addition to SDM including the Oracle database and BI Publisher components. The Oracle session delivery product plugin must be added to Oracle Communications Session Delivery Manager before performing the Report Manager installation.
Route Manager User Guide	Provides information for updating local route table (LRT) data on a single device or multiple devices.

Table   Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	Provides the following administration information: • Implement SDM on your network as a standalone server or high availability (HA) server. • Login to the SDM application, access GUI menus including help, customize the SDM application, and change your password. • Access the product plugin service through the GUI to manage product plugin tasks, including how product plugins are uploaded and installed. • Manage security, faults, and transport layer security certificates for east-west peer SDM server communication, and southbound communication with network function (NF) devices. • Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems. • Monitor SDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics. • Maintain SDM server operations, which includes database backup and database restoration and performing server cluster operations. • Use available SDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the SDM server.
Installation Guide	Provides the following installation information: • Do pre-installation tasks, which include reviewing system requirements, adjusting linux and firewall settings, completing SDM server settings and configuring your NNCentral account for security reasons. • Do the typical installation to perform the minimal configuration required to run the SDM server. • Do the custom installation to perform more advanced configurations including the mail server, cluster management, Route Manager, transport layer security (TLS), and Oracle database configuration.
Release Notes	Contains information about the administration and software configuration of the SDM feature support new to this release.
Security Guide	Provides the following security guidelines: • Use guidelines to perform a secure installation of SDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines. • Review Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system. • Follow a checklist to securely deploy SDM on your network and maintain security updates.
REST API Guide	Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a network service orchestrator (NSO), to interact with SDM and its supported product plugins.
SOAP API Guide	The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programing model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the SDM server and data structures that are used as input and output parameters for these operations.

Revision History

Date	Description
July 2018	Initial release
December 2018	• Changes topic name "Creating a Canned Report" to "Schedule a Report in BI Publisher" and changes existing topic name "Schedule a Report in BI Publisher" to "Schedule a Recurring Report in BI Publisher". • Adds "Add an Email or SMTP Server to BI Publisher" topic.

1
Overview

The Report Manager allows you to schedule and run dynamic reports on devices in your network. Currently, the Report Manager uses Oracle BI Publisher to render reports based on metrics collected from Historical Data Recording (HDR).

HDR refers to a group of management features that allow you to configure the managed device to collect statistics about system operation and function. The Report Manager collects raw data in CSV files from designated devices. This data is aggregated into time hourly, daily, weekly and monthly segments, and made available for running reports.

When you set collection parameters for a device, you can specify the type of data for collection. A collection group is a collection of devices from which the user wants to collect the same set of HDR groups. This data is organized into report types such as hardware or other HDR collection groups.

> ⬥ **WARNING:**
>
> To register BI Publisher with Oracle Communications Session Delivery Manager, see the *Register BI Publisher* chapter of the Report Manager Installation Guide.

Report Manager Prerequisites

The following prerequisites are required before you can access and use Oracle® Communications Report Manager in the Session Delivery Manager GUI :

- You must install the Session Delivery Manager server before you can install your product plugin through the Session Delivery Manager GUI. See the *Oracle Communications Session Delivery Manager Installation Guide, Release 8.1* for Session Delivery Manager server installation instructions.

- You must upload and install the product plugin. This plugin adds Report Manager to the Session Delivery Manager. Once the plugin is added, the **Report Manager** slider appears. See the *Session Delivery Manager Software Distribution Media* section in the *Oracle Communications Session Delivery Manager Release Notes, Release 8.1* for the file name of your product plugin, and the *Oracle Communications Session Delivery Manager Administration Guide* for product plugin upload and installation instructions.

2
Data Services

This chapter provides information about how data is handled between Oracle Communications Session Delivery Manager and your devices.

> **Note:**
>
> See the Configure Report Manager to Run Reports chapter for configuration information.

Pushing Data to the Session Delivery Manager Server

A device pushes historical data recording (HDR) data to the configured push receiver in standard CSV format.

Report Manager periodically monitors the push receiver folder, which is configured in Report Manager, for any new data. A push receiver is an FTP or SFTP destination server to which a device pushes records. The device creates a FTP an SFTP connection to the push receiver, or server, and the CSV files are pushed to the SDM server that is running the Report Manager application. If the server is a node of an SDM cluster, device data is delivered to each member in the cluster.

> **Note:**
>
> If a device is removed in SDM by deleting the network function (NF) to which it belongs, you can stop the sampling and pushing of HDR data from this device to SDM by logging into the device ACLI and using the **request collection stop all** command.

File Types and Naming Conventions

Statistical records are forwarded from the device to the SDM server for viewing in a comma-separated value (CSV) file. Before a file is pushed by the device, the device creates a directory by group name for which the statistic belongs (for example, diameter director, system, etc.), if the directory does not exist from a previous push.

Each file is formatted as `<UTC timestamp in seconds>.csv` (for example, 201112250000.csv).

Each CSV file contains a record for the header containing the statistical attribute name, as well as both the push interval and collection interval records. The first record of each file is a header containing the attribute name. For example, in the "System" directory, a file name of 201112250000.csv can contain the header names of CPU Utilization, Memory Utilization, Health Score, Redundancy State, etc. Also included in the files are both the push interval and collection interval files. For example, if the collection interval is one minute, and the push

interval is 15, a collection occurs every minute for 15 minutes. The CSV file in this example contains 15 records.

Aggregating Data

The configured push receiver uses FTP/SFTP to push the CSV files to the SDM server on which the Report Manager application runs. Before Report Manager can aggregate the data, it must identify new files, add them to a files table, and load them into the reporting database.

Data Type Aggregation Behavior

Below is a table of data types, and the aggregation behavior for each type.

Data Type	Aggregation Behavior
Dimension	Dimensions cannot be aggregated
Identifiers	Identifiers cannot be aggregated
State	The most recent state value
Boolean	The most recent boolean value
Count	The sum of the integer values
Range (i.e. 0-100)	The average of all values
Current value	The average of all values
Capacity	The average of all values
Index	The most recent index value
High water mark	The maximum value
Maximum rate	The maximum value
Low water mark	The minimum value
Minimum rate	The minimum value
Percentage	The average of all percentage values
Rate	The average of all rate values
Latency	The average of all latency values
Ratio	The average of all ratios
Speed	The average of all speeds
Temperature	The average of all temperatures

Time Granularity

Time Measurements in Report Manager

Report Manager time measurements are based on the UTC time. The devices pushing data to Oracle® Communications Report Manager send raw data in UTC time. UTC does not operate on Daylight Savings Time (DST), and therefore the timestamps of CSV files do not fluctuate due to DST. Time zones of the server on which the Oracle® Communications Report Manager application runs nor the reporting device are relevant in Report Manager.

Reports are available in the following time granularities: hourly, daily, weekly and monthly.

The aggregation schedule below describes the time frame for processing data based on UTC time.

- CSV Timestamps: CSV data files are titled with the UTC timestamp in seconds, otherwise known as the Unix Epoch time.

- Aggregation and Purging: Aggregation time granularities and purging schedules are based on the Gregorian calendar. References to start time and date are based on the UTC time relative to the Gregorian calendar.

Time Granularity Start and End Date

The table below describes the collection and aggregation periods of data in the Report Manager:

Time Granularity	Aggregation Schedule
Hourly	Starts at the 00 minute of the hour and ends at minute 59 of the hour. The next hour starts at the following 00 minute.
Daily	Starts at the 00:00 hour and minute of the day (midnight), and ends at hour and minute 23:59. The next day starts at the following 00:00 hour.
Weekly	Starts at the 00:00 hour and minute on the first week of the month, and ends at hour and minute 23:59 on the last day of the week. The next week starts at the following 00:00 hour.
Monthly	Starts at the 00:00 hour and minute on the first day of the month, and ends at hour and minute 23:59 on the last day of the month. The next month starts at the following 00:00 hour.

Shared Data Between Time Granularities

Aggregated data for each time granularity is independent of other granular data. Data for a given calendar week (Sunday through Saturday) can be included in reports for two consecutive calendar months if a new month begins in the middle of the week.

Purging Data

Oracle® Communications Report Manager performs a nightly purge of all expired data, CSV files, and reports based on configured data retention times.

3

Configure Report Manager to Run Reports

You can perform the following administration tasks in Oracle® Communications Report Manager so that reports can be run:

- Create new user group(s) with the application permissions necessary for these users to execute reports.

- Add users to the new user group(s) that you created.

- Add devices (that are created in Device Manager) to collection groups. Once collection group parameters are specified, Oracle® Communications Report Manager can collect data and provide reports.

- Configure a data retention policy for saving the collected data.

Add a User Group

You can add a user group to which you assign users later. Those users in turn, inherit the group-based privileges that you copy from default user groups.

1. Expand the **Security Manager** slider and select **User management**, **Groups**.

2. In the **User Groups** pane, click **Add** to add a new user group.

3. In the **Add Group** dialog box, complete the following fields:

Group name field	The user group name. Use the following guidelines for naming this group: • Use a minimum of three characters and maximum of 50. • The name must start with an alphabetical character. • You are allowed to use alphanumeric characters, hyphens, and underscores. • The user group name is case insensitive. • The user group must be unique.
Group permissions copy from drop-down list	Choose from the following default user groups to copy their privileges: • **None**—Manually configure privileges for this user group. • **administrators**—This super user group is privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups.

- **provisioners**—This group is privileged to configure Report Manager and save and apply the configuration with the exception of a LI configuration.

- **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Report Manager, and has the fewest privileges.

4. Click **OK**.

5. In the success dialog box, click **OK**.

6. Click **Back** to return to the **User Groups** table.

Apply User Group Privileges for Applications

1. Expand the **Security Manager** slider and select **User Management**, **Groups**.

2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.

3. Select the **Applications** tab and click to expand the **Applications** folder.

4. Select any folder or folder item row that are described in the table below that you want to modify and click the **Privileges** column to activate the drop-down list.

   Select the following privilege from the **Privileges** drop-down list:

   - **Full**—Enable GUI elements (such as tabs) to perform configuration operations.

   - **View**—View information only.

   - **None**—Disable configuration operations and make them disappear from the GUI.

   > **Note:**
   >
   > You must set the **Execute Reports** item privilege level to **Full**. See the table below for more information.

Application folder	Set privilege levels for all application operations.
Report Manager folder	Set privilege levels for all reporting operations accessible on the **Report Manager** slider.
Execute Reports item	You must set the privilege level for users belonging to a group to run reports full privileges so that collection reports can be configured.
Administration folder	Set all administration privileges for **Oracle Communications Report Manager**.
Configure Retention Policy item	Set privilege levels for a user group to create a retention policy for retaining Historical Data Recording (HDR) data over a period of time.
Register BI Publisher item	Set privilege levels for the **Oracle Communications Report Manager** to register with the **Oracle**

	Communications Session Delivery Manager before creating and running reports.
Plugin Management folder	Set administrative privileges for plugin management.
Actions item	Set plugin action privileges for a user assigned to the Plugin Management group to perform upload, install, uninstall, edit, delete, and recover actions.

5. Click **Apply**.

Add a User

1. Expand the **Security Manager** slider and select **User Management**, **Users**.

2. In the **Users** pane, click **Add**.

3. In the **Add User** dialog box, complete the following fields:

Group section **Assigned group** drop-down list	Choose from the following pre-existing user groups: • **administrators**—This super user group privileged to perform all operations. • **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • **provisioners**—This group is privileged to configure Oracle® Communications Report Manager and save and apply the configuration with the exception of a LI configuration. • **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle® Communications Report Manager, and has the fewest privileges.
User information **User name** field	The name of the user using the following guidelines: • Use a minimum of 3 characters and maximum of 50 characters. • The name must start with an alphabetical character. • The use of alphanumeric characters, hyphens, and underscores are allowed. • The name is case insensitive. • The name cannot be the same as an existing group name.
User information **Password** field	The password is entered for this user using the following password rules guidelines: • The password must be at least 8 characters long.

ORACLE®

- Use at least one numeric character from 0 to 9 in the password.

- Use at least one alphabetic character from the English language alphabet in the password.

- Special characters include {, |, }, ~, [, \,], ^, _, ', :, ;, <, =, >, ?, !, ", #, $, %, &, `, (,), *, +, ,, -, ., and /

User information **Confirm password** field	The same password entered again to confirm it.
User account expiration dates **Account** field	Uncheck the check box to change the user account expiration date. Click the calendar icon to open a calendar to choose the date after which the user account expires. **Note:** If the check box is checked (default) the user account never expires.
Password expiration dates **Password** field	Uncheck the check box to change the password expiration date. Click the calendar icon to open a calendar to choose the date after which the user password expires. **Note:** If the check box is checked (default) the password never expires.

4. Click **OK**.

   The following information displays in the **Users** table:

User name column	The user name.
Group column	The user group to which the user belongs.
Status column	The status of the user account is either **enabled** or **disabled**.
Operation status field	The state of the user account and its expiration date: • **active**—The account is valid and the user can log in. Neither the account nor password expiration dates have been exceeded. • **account expired**—The account expiration date has expired. • **password expired**—The password expiration date has expired.

- **password deactivated**—The failed login attempts by the user exceeded the allowed number of tries as specified by the value set for password reuse count parameter in password rules.

- **locked out**—The user has exceeded the login failures and the account is disabled until the lockout duration has passed.

Collect Data for Devices or Device Groups

Add a Device Group

Use the following naming conventions when you add a device group:

- It must start with an alphabetic character.

- It can contain a minimum of three characters and a maximum of 50 characters.

- It can contain the following characters: alphabetic, numeric, hyphens (-), and underscores (_).

- It can be a mix of upper-case and lower-case characters.

- It cannot contain symbols or spaces.

- It cannot be the same name as an existing group name within the same level in the hierarchy (sibling).

1. Expand the **Device Manager** slider and click **Device Groups**.

2. In the **Device Groups** pane, click **Add**.

3. In the **Add device group** dialog box, enter the name for the device group in the **Device group name** field and click **OK**.

   The device group now appears in the **Device Groups** pane.

Add a Network Function with Devices

Use this task to add a network function (NF) with devices to the default **Home** group or a group that you created. Once the NF is added successfully, the Oracle® Communications Report Manager plug-in is able to communicate with the devices in the NF.

Pre-requisite: If you are not using the default **Home** group to add an NF, you must specify a group for the NF.

1. Expand the **Device Manager** slider, and click **Devices**.

2. In the **Managed Devices - Group View** pane, select a group, and click **Add**.

3. In the **Select Network Function Type** dialog box, click the element manager (EM) product plugin category from the **Categories** table that manages your devices.

4. In the **Network Function Type** drop-down list, select from the following NF types:

   - **Device**—A NF that contains a single standalone device or device high-availability (HA) pair.

   - **Device Cluster**—An NF that contains a device cluster that shares a common, top-level offline configuration template.

> **✏ Note:**
>
> Oracle Communications Report Manager does not currently support device clustering.

5. Click **Continue**.

6. In the **Add Network Function: Device** dialog box, complete the following fields:

Network Function Name field	The Network Function (NF) name that you want to use for the device(s) that you are configuring.
Primary IP address field	The primary IP address for this device.
Secondary IP address field	The IP address for the second device, if this device is part of an HA pair.
User Name field	The device user name.
User Password field	The device password.
LI encryption password field	(Hidden) The Lawful Intercept (LI) encryption password for the LI configuration. This field appears if the LI administrator is logged into Oracle Communications Session Delivery Manager. This parameter is not available for the Enterprise Edge and Core plug-in at this time.
SNMP agent mode drop-down list	Select the SNMP version number that the SNMP agent supports and click **Load**. Valid versions are **v1**, **v2** and **v3**. If you select **v3**, authentication fields for SNMP version 3 appear. See below for more information about these fields. When you add a device, you must specify whether to manage the device using SNMPv1, SNMPv2, or SNMPv3. The SNMP version cannot be changed for an existing device once it is added unless the device is removed and added again later.
SNMP port field	The SNMP port number. The default SNMP port number is 161.
SNMP community name field	The SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information. This field applies only to SNMP version 1 and 2. The SNMP community must be configured on the device before adding the device to the Session Delivery Manager. Use the device CLI to configure the **ip-addresses** parameter found in the **configure terminal** > **system** > **snmp-community** element. For more information, See the device product documentation for more information.

SNMPv3 user name field	The SNMP version 3 user name.
SNMPv3 authentication protocol drop-down list	Select the SNMP version 3 authentication protocol: • **SHA**—Secure hash algorithm (SHA-1). • **MD5**—MD5 hash algorithm. • **NONE**
SNMPv3 authentication password field	The SNMP version 3 authentication password.
SNMPv3 privacy protocol drop-down list	Select the SNMP version 3 privacy protocol: • **DES**—Data encryption standard algorithm (DES) for the encryption of electronic data. • **AES128**—Advanced encryption standard (AES) encryption algorithm. • **NONE**
SNMPv3 privacy password field	The SNMP version 3 privacy password.

7. Click **Apply**.

The NF and its associated device(s) or the NF with the associated device(s) appear in the **Managed Devices** table.

Add a Collection Group

Pre-requisites: Oracle® Communications Report Manager must be installed properly and the reporting service must be operational. See the *Oracle® Communications Report Manager Installation Guide* for more information.

> **Note:**
>
> All devices that are added to a collection group must be running the same software and platform version.

1. Expand the **Report Manager** slider and select **Reports**, **Collection Groups** from the navigation pane.

> **Note:**
>
> You must have the proper user privileges in order to see the **Collection Groups** option in the **Reports** folder on the navigation pane. See the previous sections in this chapter for more information.

2. In the **Collection Groups** pane, click **Add**.

3. In the **Add a Collection Group** pane (Step 1 of 3), complete the following fields:

Name field	The collection group name.
Description drop-down list	The description of the collection group.
Start collection field	Select the **Now** checkbox to start the collection of data now.
Later	Click the calendar icon to select a future start date. Enter the future time hh:mm:ss
Stop collection field	Select the **Never** checkbox to stop data collection through manual intervention by using the **Stop Collection** button.
At	Click the calendar icon to select a definitive end date. Enter the definitive end time: hh:mm:ss

4. In the **Managed Devices** table, navigate to select individual devices, or navigate to an entire device group folder from which you want to collect data.

5. Click **Add** to move the device(s) or device group(s) to the **Collect on following devices** table.

6. Click **Next**.

7. In the **Add a Collection Group** dialog box (Step 2 of 3), complete the following fields:

Push interval field	The number of minutes from 1 to 120 for how often you want the device to send collected records to the push receiver. The default time is 15 minutes. A push receiver is an FTP or SFTP destination server to which a device pushes records.
Global Collection interval field	The number of minutes you want the device to collect statistics for the specified historical data record (HDR) groups (used for data detection) to view in a report; this value cannot exceed the push interval value. The default time is 5 minutes.
Collect on all groups field	Select the **Yes** checkbox to collect data on all collection groups.

8. Check the checkbox for each collection group that you want to change in the **Specify the collection interval for each device group, if different than global interval** table (if a device group needs a different collection interval than the global collection interval value, which is 5 minutes by default).

9. Click **Next**.

10. In the **Add a Collection Group** dialog box (Step 3 of 3), complete the information required to configure the SFTP protocol for pushing HDR data:

FTP Server IP Address field	The IP address or hostname for the FTP/SFTP push receiver server.
User name field	The user name for the host FTP/SFTP user.
Password field	The password for the host FTP/SFTP user.
FTP path for data storage field	The directory on the push receiver where you want data placed, which may differ from the absolute path given system security though the two typical points to the same location.

	Protocol drop-down list	Select **FTP** or **SFTP** as the protocol to send CSV files. You must generate a host key from the push receiver server (the SDM server) and export it to the device(s) if the selected protocol is SFTP. See the Additional Steps for Configuring a Collection Group that Uses SFTP section for more information.
	Absolute path of data storage field	The absolute (Oracle Communications Session Delivery Manager server) path for data storage, which can point to the same directory as the FTP path. For example: **/home/nncentral/hdrdata** In some implementations absolute path may need to include the FTP root directory. For example: <ftpRootDirectory>/<ftpLocation>

11. Click **Finish** to complete collection group configuration.

12. In the success message that appears, click **OK**.

    The collection group now appears in the **Collection Groups** table.

Additional Steps for Configuring a Collection Group that Uses SFTP

If you add a collection group and you select **SFTP** for the protocol that is used for sending CSV files, you must use this task to generate a host key from the push receiver (SDM server) and export it to the device(s).

See the Add a Collection Group section for more information.

1. Log in to the SDM server as the root user.

   ```
   su root
   ```

2. Change to the ssh directory. For example:

   ```
   /etc/ssh
   ```

3. Enter the **ssh-keygen -e** script.

4. When prompted, enter the following path for the generated host key:

   ```
   /etc/ssh/ssh_host_dsa_key.pub
   ```

5. Copy the base64 encoded public file making sure in include the BEGIN and END markers as they are specified by RFC 4716 (The Secure Shell (SSH) Public Key File Format). For example:

   ```
   --- BEGIN SSH2 KEY ---
   <generated public key>
   --- END SSH2 KEY ---
   ```

6. Log into the device that is communicating with SDM using SFTP and access the CLI.

7. From admin mode use the **ssh-pub-key** command to import the host key to the device.

   For importing a host key, this command takes the format:

   ```
   ORACLE# ssh-pub-key import known-host <sdm_server_name>
   ```

8. Paste the host key with the bracketing BEGIN and END markers at the cursor point.

9. Enter a semi-colon (**;**) to signal the end of the imported host key.

10. Follow directions to save and activate the configuration. For example, the entire import sequence is shown below:

```
ORACLE# ssh-pub-key import known-host fedallah
IMPORTANT:
 Please paste ssh public key in the format defined in rfc4716.
 Terminate the key with ";" to exit.......
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "2048-bit RSA, converted from OpenSSH by klee@acme54"
AAAAB3NzaC1yc2EAAAABIwAAAQEA7OBf08jJe7MSMgerjDTgZpbPblrX4n17LQJgPC7clL
cDGEtKSiVt5MjcSav3v6AEN2pYZihOxd2Zzismpoo019kkJ56s/IjGstEzqXMKHKUr9mBV
qvqIEOTqbowEi5sz2AP31GUjQTCKZRF1XOQx8A44vHZCum93/jfNRsnWQ1mhHmaZMmT2LS
hOr4J/Nlp+vpsvpdrolV6Ftz5eiVfgocxrDrjNcVtsAMyLBpDdL6e9XebQzGSS92TPuKP/
yqzLJ2G5NVFhxdw5i+FvdHz1vBdvB505y2QPj/iz1u3TA/3O7tyntBOb7beDyIrg64Azc8
G7E3AGiH49LnBtlQf/aw==
---- END SSH2 PUBLIC KEY ----
;
SSH public key imported successfully....
WARNING: Configuration changed, run "save-config" command to save it
and run "activate-config" to activate the changes
ORACLE# save-config
checking configuration
-----------------------------------------------------------------
...
...
...
-----------------------------------------------------------------
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
ORACLE# activate-config
Activate-Config received, processing.
waiting for request to finish
SD is not QOS-capable
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
ORACLE#
```

11. Enter the **show security ssh-pub-key** command to verify the host key.

12. Repeat steps 6 through 11 to import the host key for additional devices.

Edit the Collection Group Start and End Times

The start and end times are the only parameters in a collection group that can be edited after a collection group is created.

1. Expand the **Report Manager**.

2. Click **Collection Groups**.

3. In the **Collection Groups** pane, select the collection group you want to edit and click **Edit**.

4. In the **Devices** tab, edit the start or end times and click **Apply**.

Change the Data Retention Policy

Once data collection has begun, the Oracle Communications Session Delivery Manager server running Oracle® Communications Report Manager aggregates the data based on several default types of periodic data collection methods. Use this task if you want to modify the default data retention policy for retaining raw data and each aggregation time (hourly, daily, weekly, and monthly). Data and reports that exceed the retention times you configure are automatically purged from the system each night.

> **Note:**
>
> There is no maximum value for retention time. If you set the retention time to 0, data is not retained for that time period, and the data is purged once it is aggregated.

> **Caution:**
>
> Increasing retention times increases disk usage. Ensure that the host to which HDR data is being delivered has the disk capacity to store the required retention periods.

1. Expand **Report Manager** and click **Retention Policy** in the navigation pane.

2. In the **Retenion Policy** table, select the retention time for raw data, hourly, daily, weekly and monthly aggregated data types, and saved reports from their respective **Store for** drop-down lists:

Retention Policy

Type	Store for
Raw data	30 days
Hourly aggregated data	720 hours
Daily aggregated data	30 days
Weekly aggregated data	52 weeks
Monthly aggregated data	12 months
Saved reports	1 months

3. Click **Apply**.

4
Reports

The Report Manager provides a small set of predefined reports. Operational reports are the reports you run on aggregated HDR. To run a report, you must first configure collection groups. Refer to the Configure Report Manager to Run Reports chapter for more information.

If you enabled **Single Sign On** when registering BI Publisher in Report Manager, select **Operational Reports** in the **Reports Manager** slider to open BI Publisher in a new tab and sign into BI Publisher with the same account name used to sign into Oracle Communications Session Delivery Manager. If you did not enable **Single Sign On**, you must log into BI Publisher manually.

> **Note:**
>
> You will not see the **Operational Reports** section under the Report Manager slider unless you are logged in as a reporting user. See the Apply User Group Privileges for Applications section for more information.

Reports in BI Publisher

The upper-case groups (e.g., Performance, QoS, Registrations, etc.) correspond to the canned reports, while the lower-case groups (e.g., radius-stats, session-agent, sip-invites, etc.) correspond to the SBC's HDR groups. For more information about HDR groups, see the HDR Resource Guide for your software version.

Run a Canned Report

Report Manager comes with the following predefined reports:

- Dashboard—Displays space used, fan speed, temperature, and voltage.
- Performance—Displays CPU, memory, registration cache, and concurrent sessions.
- QoS—Displays RFactor, major exceeded, critical exceeded, and successful sessions.
- Registrations—Displays total registrations, initial registrations, refresh registrations, and de-registrations.
- Security—Displays ACL entries, requests and message status, ACL entry promotions and demotions, and demotions.
- Session Realm—Displays calls per second, QoS RFactor, answer seizure ratio, and one-way signalling latency.
- Summary—Displays sessions, session state, dialogs, and errors.

1. In the toolbar, click **Catalog**.
2. In the **Folders** section, navigate to **Shared Folders**, **OCSRM**, **Reports**.
3. Select one of the following folders:

- **Dashboard**

- **Performance**

- **QoS**

- **Registrations**

- **Security**

- **Session Realm**

- **Summary**

4. To run the report, select Open under the time granularity you want (Daily, Hourly, Monthly, Yearly).

> **Note:**
>
> If hourly summary reports are not displaying, see "Hourly Summary Reports" in *Report Manager Installation Guide for Oracle Fusion Middleware 12c*.

5. To schedule a report, click **Schedule**.

6. To manage the job or edit start and end times, click **Jobs**.

7. To view the job history, click **Job History**.

8. To add the report to your Favorites, click **More**, **Add to Favorites**.

Create a Data Model

Use this task to create a data model that is later used for a BI Publisher Oracle Communications Session Delivery Manager Report.

> **Note:**
>
> See the BIP product page for more options for creating data models.

1. Login to Oracle Communications Session Delivery Manager as a reporting user and select **Report Manager**, **Operational Reports**.

> **Note:**
>
> You must be logged in as a reporting user to view the **Operational Reports** selection under the Report Manager. Refer to the Apply User Group Privileges for Applications section for more information.

A new browser tab displays the BI Publisher Enterprise page.

2. On the **BI Publisher Enterprise** login page, enter the user name and password credentials.

3. On the **BI Publisher Enterprise** page, select **Create**, **Data Model** to create a new data model.

4. In the **Data Model** navigation pane, select **Data Model**, **Data Sets** and select **SQL Query** from the **Diagram** tab.


5. In the **New Data Set - SQL Query** dialog box, complete the following fields:

|	
Name field	The name of the new data set. For example, Hourly Session Realm Stats.
Data Source drop-down list	Select **ocsrm**. The **ocsrm** data source is what is used to connect to the OCSDMDW Oracle Database instance through JDBC connection.

6. Next, in the **New Data Set - SQL Query** dialog box, click **Query Builder** to build your SQL query. For example:
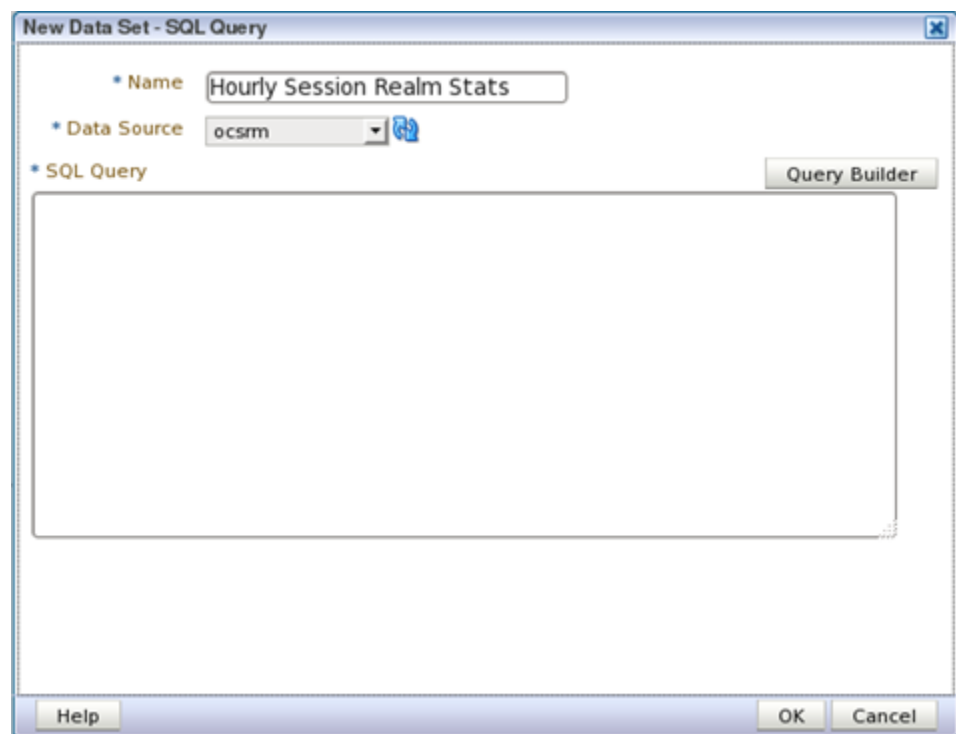
7. In the query builder tool (refer to the illustration in step 8), select **OCSREMDW** from the **Schema** drop-down list, which is the Oracle database schema that contains the tables that contains the HDR raw and aggregated data sets for the device.

8. In the **Search** field, enter the table name for which you are searching. In the example below, a table prefixed T_HOURLY_* indicates that the data is aggregated in hourly increments, a table prefixed T_DAILY_* indicates that the data is aggregated in daily increments, and so on.
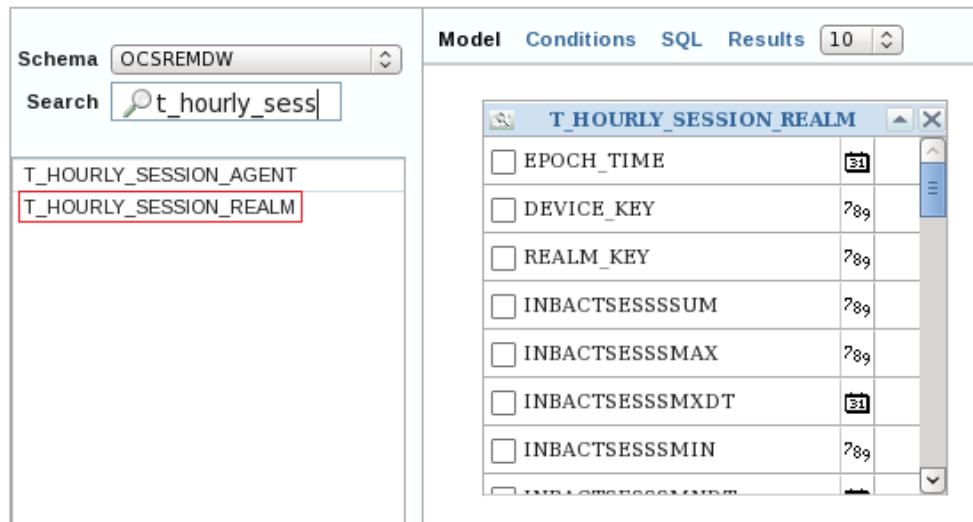

9. Scroll through the selected table columns and check the desired boxes for the data set. For example:
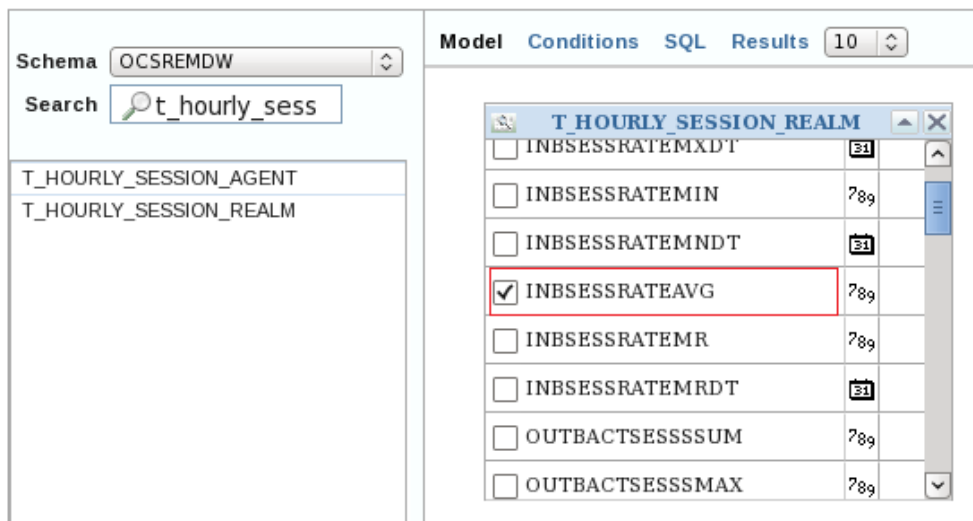
10. In the **Search** field, enter the **D_DEVICE** table.

11. Join the two tables that appear by matching the **DEVICE_KEY** (primary key) row from both tables by clicking on the grey box to the right of the DEVICE_KEY row in each table. The black arrow shows a blue line joining the two tables after they are they are connected successfully. For example:
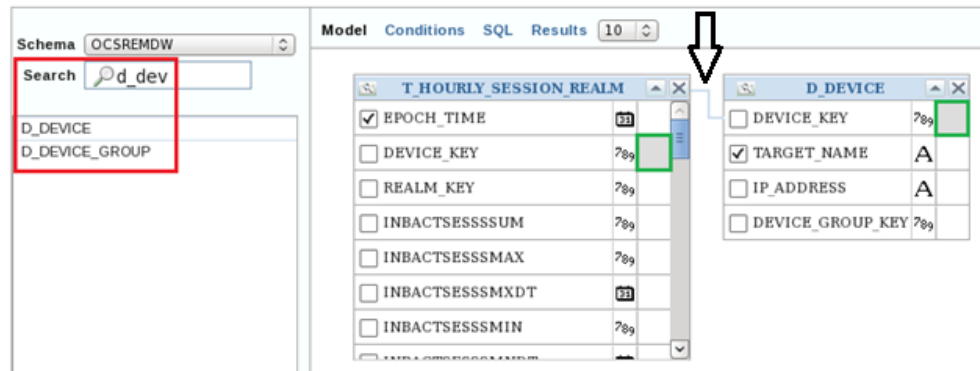
12. In the **Search** field, enter the **D_REALM** table.

13. Join the two tables that appear by matching the **REALM_KEY** (primary key) row from both tables by clicking on the grey box to the right of the REALM_KEY row in each table. The blue line joins the two tables after they are they are connected successfully. For example:
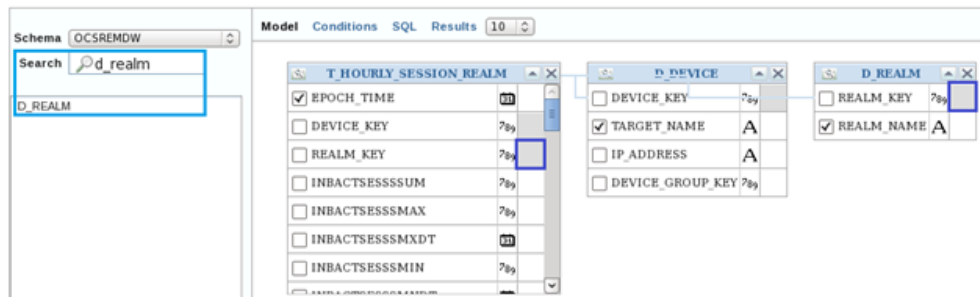
14. Check all the check boxes with the desired data columns.

15. Click **Save** to exit the query builder tool.

16. In the **New Data Set - SQL Query** dialog box, click **OK**.

    A data model is successfully created.

Create a Filter for a Session Delivery Manager Report: Example

The following example is used to create a filter with a device group, list of values, and device parameters for an Oracle Communications Session Delivery Manager report. The filter name is displayed as a drop-down list item in the report using the data model you added in the previous section.

> **Note:**
>
> The SQL queries must be entered exactly as they are shown in the following steps if you are going to use this example.

1. In the **Data Model** navigation pane, click **List of Values**.

2. In the **List of Values** pane, click the plus (+) icon above the table to create a new list of values in the table.

3. In the new table row under the **Name** column, enter the name **devices**.

> **Note:**
>
> Ensure that the **Type** drop-down list is set to **SQL Query** and the **Data Source** drop-down list is set to **ocsrm** for this step and subsequent steps.

4. In the SQL query box below the table, enter the following SQL query:

```
select      d_device.target_name as target_name
 from     ocsremdw.d_device_group d_device_group,
    ocsremdw.d_device d_device
 where   d_device.device_group_key=d_device_group.device_group_key and
device_group_name in ( :device_group)
```

5. In the **List of Values** pane, click the plus (+) icon again to create another list of values in the table.

6. In the next table row under the **Name** column, enter the name **realms**.

7. In the SQL query box below the table, enter the following SQL query:

```
select d_realm.realm_name as realm_name
 from ocsremdw.d_realm d_realm
```

8. In the **List of Values** pane, click the plus (+) icon again to create another list of values in the table.

9. In the next table row under the **Name** column, enter the name **device_groups**.

10. In the SQL query box below the table, enter the following SQL query:

```
select      d_device_group.device_group_name as device_group_name
 from     ocsremdw.s_nnc_user s_nnc_user,ocsremdw.s_nnc_user_group
s_nnc_user_group,
    ocsremdw.d_device_group d_device_group
 where   s_nnc_user_group.device_group_name=d_device_group.device_group_name
 and     s_nnc_user_group.nnc_user_group_name=s_nnc_user.nnc_user_group_name
and upper(nnc_user_name)=upper(:xdo_user_name)
```

Once the list of values for devices, realms, and device groups is configured, the **List of Values** pane appears. For example:
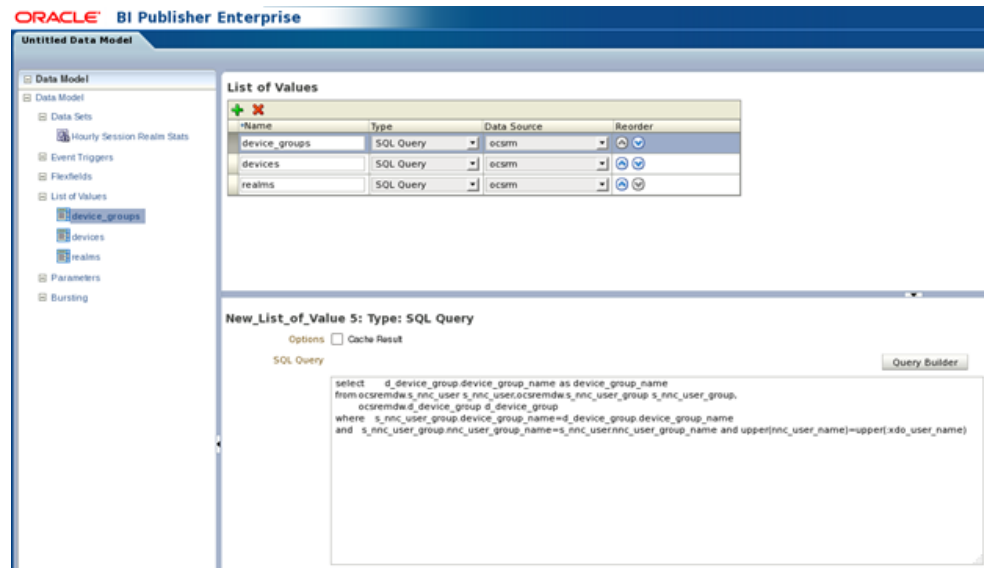
11. In the **Data Model** navigation pane, click **Parameters**.

12. In the **Parameters** pane, click the plus (+) icon above the table to create a parameter in the table.

13. In the new table row under the **Name** column, enter the name **device_group**, select **Menu** from the **Parameter Type** drop-down list and complete the following fields:

Display Label field	Enter **Device Group** as the label for this parameter.
List of Values drop-down list	Select **device_groups**.
Number of Values to Display field	Enter **100**.
Options check box	Select from of the following check boxes: • **Multiple Selection** • **Can select all** • **Refresh other parameters on change**

14. In the **Parameters** pane, click the plus (+) icon above the table to create a parameter in the table.

15. In the new table row under the **Name** column, enter the name **start_date**, select **Date** from the **Data Type** drop-down list, select **Date** from the **Parameter Type** drop-down list, select **2** from the **Row Placement** drop-down list and complete the following fields:

Display Label field	Enter **Start Time** as the label for this parameter.
Date Format String field	Enter **MM-dd-yyyy hh:mm**.

16. In the **Parameters** pane, click the plus (+) icon above the table to create a parameter in the table.

17. In the new table row under the **Name** column, enter the name **end_date**, select **Date** from the **Data Type** drop-down list, select **Date** from the **Parameter Type** drop-down list, select **2** from the **Row Placement** drop-down list and complete the following fields:

Display Label field	Enter **End Time** as the label for this parameter.

| Date Format String field	Enter **MM-dd-yyyy hh:mm**.

Once the list of parameter values is configured, the **Parameters** pane should appear as shown below:
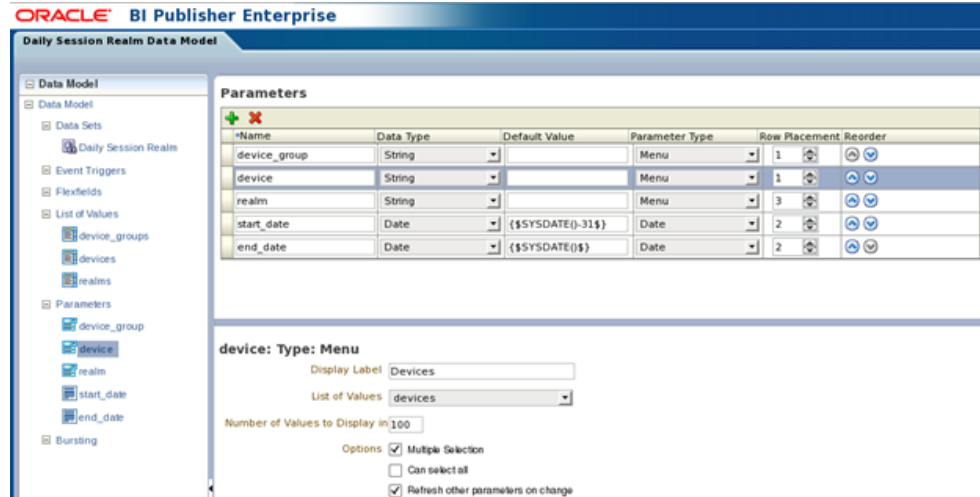
18. In the **Data Model** navigation pane, select **Data Sets** > **Hourly Session Realm Stats** as shown in the **Untitled Data Model** window below:

19. In the pre-populated **Edit Data Set - Hourly Session Realm Stats** dialog box, enter the text shown in the red box in the figure below after the existing text in the SQL Query box:
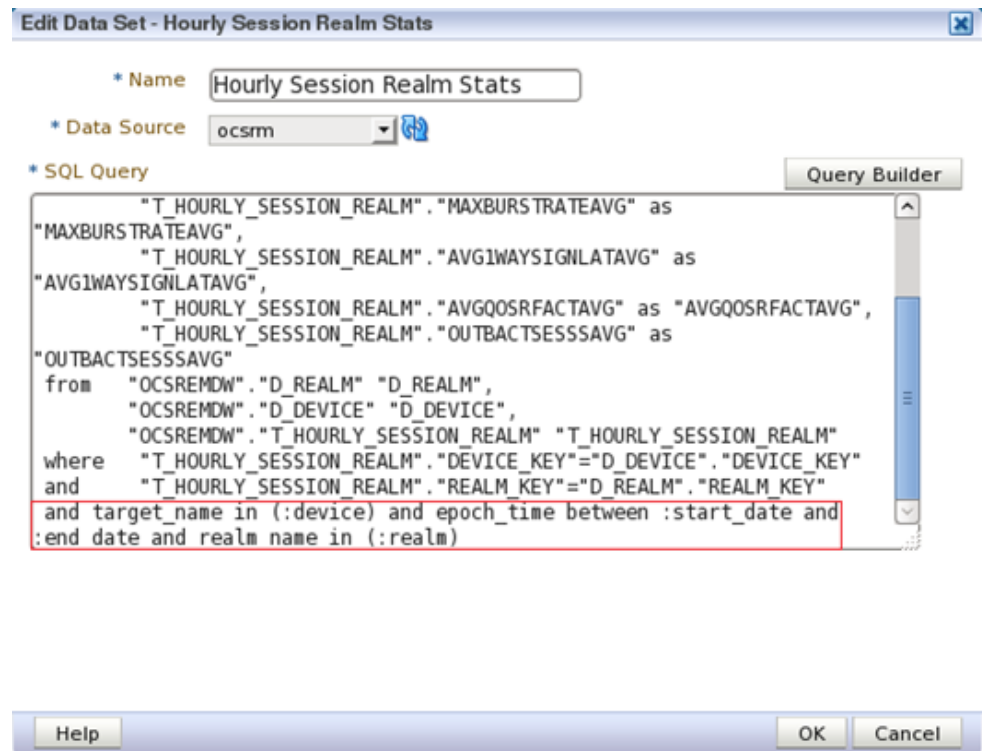
The line you entered joins the parameters that you created in the previous stems and filters the resulting query based on the devices, realms, start, and end dates selected in the report.

20. Click **OK**.

21. In the Untitled Data Model screen, click the save (disk) icon on the top right side of the window and save the data model. For example, you can name it "Hourly Session Realm Stats Data Model."

22. After you successfully save the data model, you can create a report called "Daily Session Realm Stats Report" using this newly created "Hourly Session Realm Stats Data Model."

Create a New Report

1. In the Create section, click **Report**.

2. If your data source is an existing data model, select **Use Data Model**, click the magnifying glass, and select an existing data model from the catalog. If your data source is in a spreadsheet, click **Upload Spreadsheet** and browse to the .xls file.

   If the uploaded spreadsheet contains multiple sheets, select the sheet to use as the data source. You can include data from only one sheet.
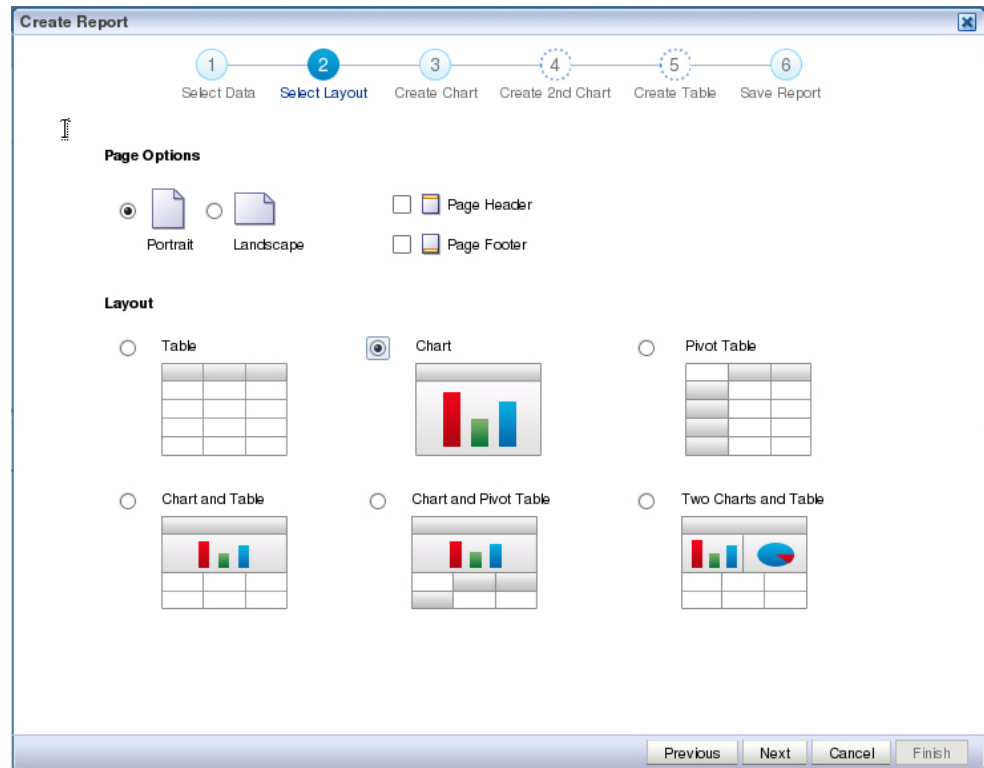   A picture of selecting a data model from the catalog is shown.
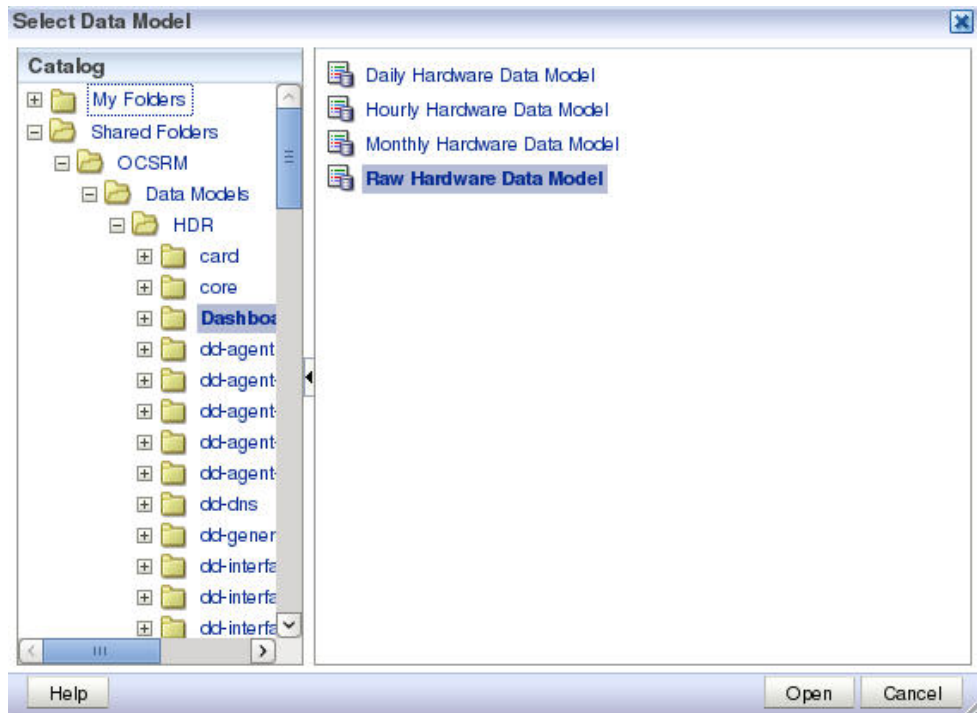
3. After selecting a data model, click **Open**.

4. Click **Next**.

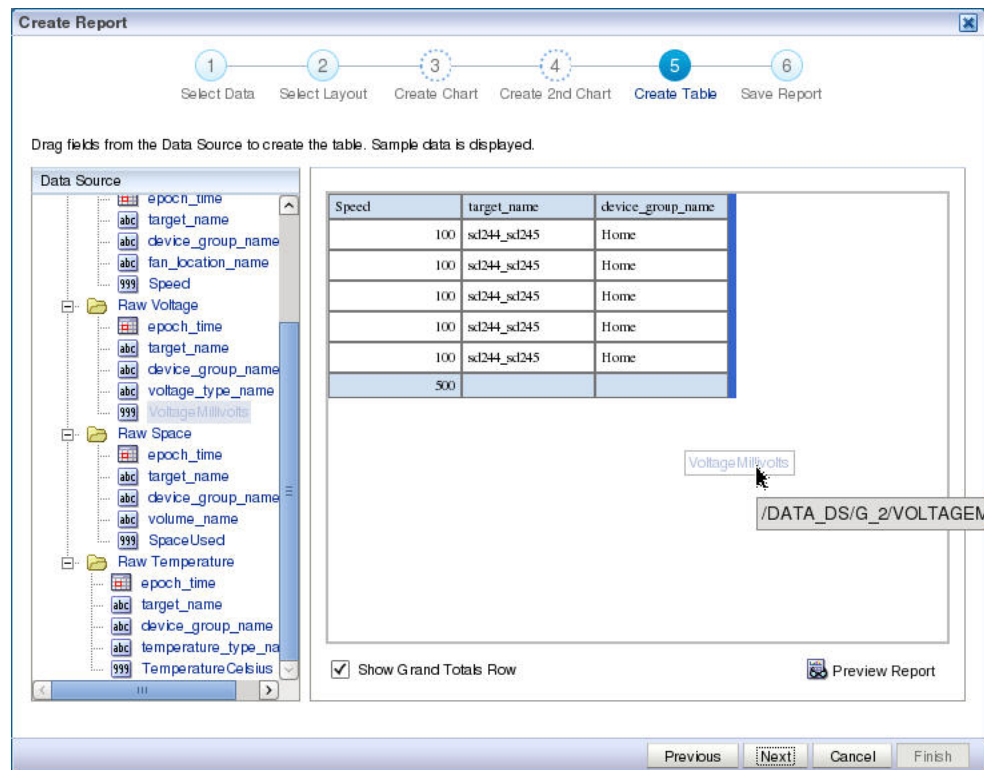5. Select a layout for your report.

   Page Options are:

   • Portrait

   • Landscape

   • Page Header

   • Page Footer

   Layout options are:

   • Table

   • Chart

   • Pivot Table

   • Chart and Table

   • Chart and Pivot Table

   • Two Charts and Table

6. Click **Next**.

7. Select the parameters you want in your table and drag them from the **Data Source** tree to the main window.


8. Select View Report and click **Finish**.

9. In the Save As dialog box, select a location to save the report and a title.

10. Click **Save**.

11. The report will begin automatically.

> ✎ **Note:**
>
> For more information about running reports, see Creating and Editing Reports from the BI Publisher documentation.

Schedule a Report in BI Publisher

1. From the **Report Manager** slider, click **Operational Reports**.

2. On the **BI Publisher Enterprise** login page, enter the user name and password credentials.

3. Click **Report Job** in the **Create** section of the **Home** tab.
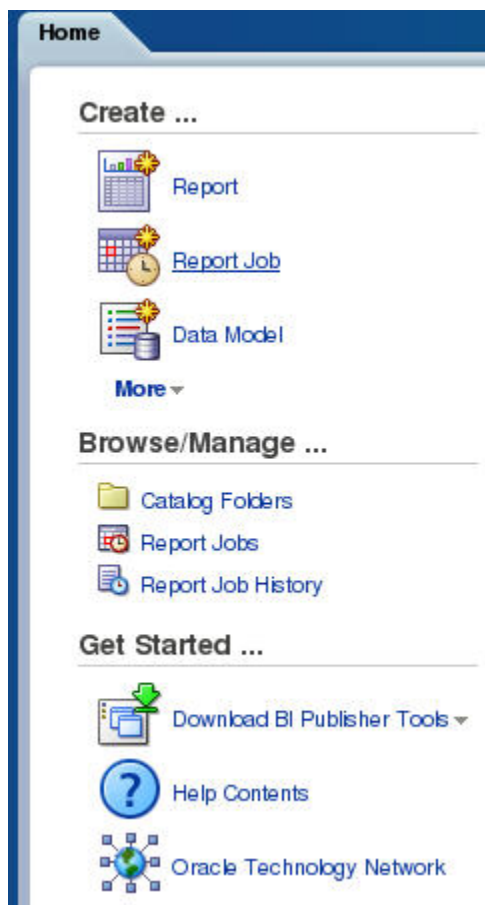
4. Click the magnifying glass icon next to the **Report** field to select a report.

5. Expand **Shared Folders**, **OCSRM**, **Reports**.

6. Select the canned report you want. Then select the time granularity you want.
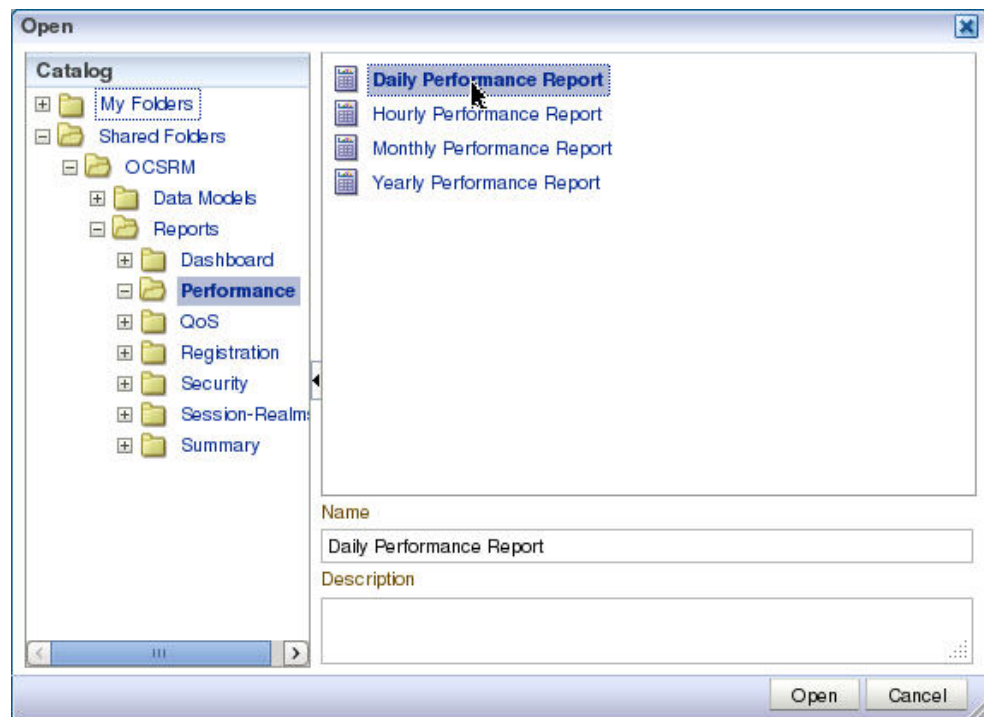
7. Click **Open**.

8. In the **Schedule Report Job** tab, click the calendar icon next to the **Start Time** field to specify the start time and click the calendar icon next to the **End Time** field to specify the end time for the report.
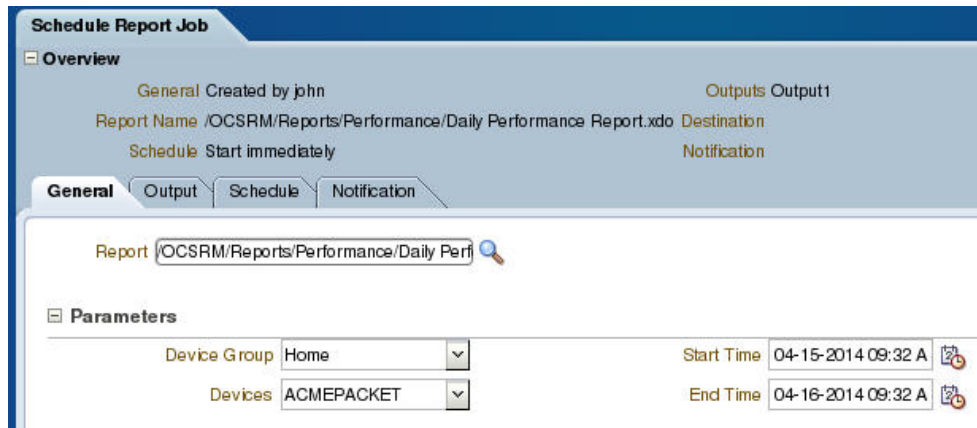
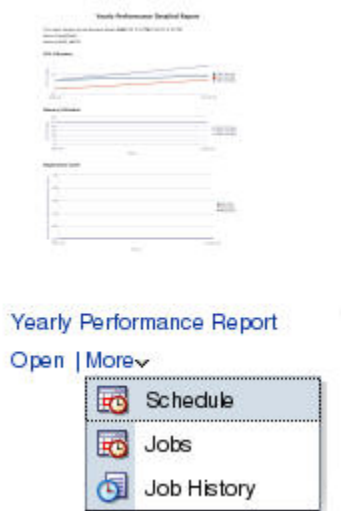9. Click **Submit** in the top right corner.

Schedule a Recurring Report in BI Publisher

After a report is created, you may schedule the report to run at regular intervals.

1. If you have already created the report, from the **Home** tab click **More**, **Schedule** under the report you want to schedule.

2. In the **Schedule Report Job** tab, select the **Schedule** tab to create a job.

3. Select the frequency from the drop-down list.

4. Select the start time and, if given, the stop time.

5. If you want to conditionally execute reports, select the Use Trigger check box and specify the relevant data model.

6. Enter a name for the report and click **OK**.

7. Click **Submit**.

Add an Email or SMTP Server to BI Publisher

1. Log in to BI Publisher and select **Administration**, **Delivery**, **Email**.

2. Click **Add Server**.

3. Enter the appropriate information for your email server and click **Test Connection**.

4. Click **Apply**.

Add Reports to a Favorites List

The Favorites region enables you to create your own list of reports for quick access. From the Favorites region you can view, schedule, configure, or edit the objects that you place there (providing you also have proper permissions).

There are several ways to add objects to the Favorites region:

• Locate the object in the catalog, click the **More** link, and then click **Add to Favorites**.

• From the Report Viewer, click the **Actions** menu, and then click **Add to Favorites**.

• Use the **Manage** link on the **Home** page to add reports.

To add and delete reports from the Favorites region, click the **Manage** link to open the Favorites area for editing.

To add a report to Favorites:

1. Click the report in the catalog pane.

2. Drag the report to the Favorites region.

To delete an object from Favorites:

1. Locate the item and click the **More** link.

2. Click **Remove**.

Links to BI Publisher Documentation

Oracle provides extensive documentation for BI Publisher.

For a quick introduction about using BI Publisher, see the BI Publisher Quick Start Guide.

For instructions on viewing and running reports, see the BI Publisher User's Guide.

If you are the system administrator for BI Publisher, please review the BI Publisher Administrator's Guide.

For a list of all BI Publisher documentation, see the BI Publisher Documentation Library.

5
Reset Passwords for Oracle and BI Publisher Database Users

The Oracle database (OCSREMDW) user password and the BI Publisher database user passwords (DEV_MDS, DEV_BIPLATFORM, NNCENTRAL) that you configured in the Report Manager installation expires after 180 days. Use the tasks in this chapter to reset any of these passwords before they expire.

Seven days before the Oracle database or BI Publisher passwords expire, an alarm displays in the **Fault Manager**, **Alarms** pane that indicates that any one of these passwords need to be reset. These alarms are prompted by the apNNCReportingPswdExpiration trap. The apNNCReportingPswdExpirationClear trap clears the warning in the pane once these passwords are reset. If you are using Report Manager in an SDM cluster, each cluster member node sends out a warning event before a password expires. However, when this warning event is cleared, the clearing event only indicates the server from which the clear trap was generated (even though the other cluster member nodes may also be in a clear state).

> **Note:**
>
> If you need to modify when to receive the notification, you can edit the BEServerConfig.xml file using the "daysBeforeExpirationToCheck" option. The file is located in the following SDM server directory:
>
> `/AcmePacket/NNC<version>/conf/BEServerConfig.xml`

Reset the Password for the Oracle Database User

1. Login to the server on which SDM is installed with the nncentral user.

   `ssh -Y nncentral@<OCSDM-Linux-server>`

2. Change directory to the SDM bin directory.

   `cd /home/nncentral/AcmePacket/NNC<version>/bin`

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

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

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

4. Go to the Oracle database bin home directory.

```
cd $ORACLE_HOME/bin
```

5. Specify the Oracle SID to ocsdmdw.

```
export ORACLE_SID=ocsdmdw
```

6. Connect to the Oracle database as the Oracle system administrator (sysdba).

```
./sqlplus / as sysdba

SQL*Plus: Release 11.2.0.1.0 Production on Tue Mar 29 10:29:14 2017

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Connected to:
Oracle Database 11g Release 11.2.0.1.0 - 64bit Production

SQL>
```

7. Check the OCSREMDW user status.

```
SQL> select username, account_status from dba_users where username =
'OCSREMDW';

USERNAME                        ACCOUNT_STATUS
------------------------------ --------------------------------
OCSREMDW                        LOCKED
```

8. If the status is in the LOCKED status (the status before the password expires) then you must unlock the OCSREMDW user account before you reset the password. If there is a different status, such as OPEN, EXPIRED and LOCKED, or EXPIRED, skip this step and proceed to step 9.

```
SQL> alter user ocsremdw account unlock;

User altered.
```

9. Reset the OCSREMDW password by entering the original password that was specified during original database installation.

```
SQL> alter user ocsremdw identified by <original password>;

User altered.
```

10. Logout as the Oracle system administrator (sysdba).

```
SQL> exit;
Disconnected from Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
```

11. Connect to OCSDMDW database as the OCSREMDW user to ensure that the database is operational.

```
./sqlplus ocsremdw/<password>@ocsdmdw

SQL*Plus: Release 11.2.0.1.0 Production on Tue Mar 29 10:43:17 2017

Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Connected to:
Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
```

```
SQL>
```

12. Logout as the OCSREMDW user.

```
SQL> exit;
Disconnected from Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
```

13. Change to the SDM server bin directory.

```
cd /home/nncentral/AcmePacket/NNC<version>/bin
```

14. Start the SDM server.

```
./startnnc.sh
```

15. Check the Reporting Service log to make sure that it was started successfully.

```
cd <OCSDM-INSTALL_DIRECTORY>/logs
grep "service started" ReportingService.log
2016-02-09 16:44:37,988 INFO
[com.acmepacket.ems.server.services.ReportingService] - Method:
[startService]
Thread: [ReportingService:25]  Msg:[...service started]
```

16. If you are running an SDM server cluster, repeat the previous steps for each cluster member node.

Reset the Password for BI Publisher Users

1. Login to the server on which the BI Publisher application is installed.

```
ssh -Y oracle@<BI-Publisher-server>
```

2. Change directory to the SDM bin directory (if the BI Publisher application is running on the same server as SDM).

```
cd /home/nncentral/AcmePacket/NNC<version>/bin
```

3. Execute the **shutdownnnc.sh** script (if the BI Publisher application is running on the same server as SDM). By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

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

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

4. Stop the WebLogic server by running the stopWeblogic.sh script.

```
cd /app/OracleMiddleWare/user_projects/domains/bifoundation_domain/bin/
./stopWebLogic.sh
```

The default user name is weblogic.

5. Go to the Oracle database bin home directory.

```
cd $ORACLE_HOME/bin
```

6. Specify the Oracle session identifier (SID).

   For example:

   ```
   export ORACLE_SID=AcmeBIPublis
   ```

7. Connect to the Oracle database as the Oracle system administrator (sysdba).

   ```
   ./sqlplus / as sysdba

   SQL*Plus: Release 11.2.0.1.0 Production on Tue Mar 29 10:29:14 2017

   Copyright (c) 1982, 2009, Oracle.  All rights reserved.

   Connected to:
   Oracle Database 11g Release 11.2.0.1.0 - 64bit Production

   SQL>
   ```

8. Check the user account status for the BI Publisher database user passwords (DEV_MDS, DEV_BIPLATFORM, or NNCENTRAL).

   For example:

   ```
   SQL> select username, account_status from dba_users where username =
   'DEV_MDS';

   USERNAME                        ACCOUNT_STATUS
   ------------------------------ --------------------------------
   DEV_MDS                         LOCKED
   ```

9. If the status is in the LOCKED status (the status before the password expires) then you must unlock the BI Publisher database user account before you reset the password. If there is a different status, such as OPEN, EXPIRED and LOCKED, or EXPIRED, skip this step and proceed to step 10.

   For example:

   ```
   SQL> alter user DEV_MDS account unlock;

   User altered.
   ```

10. Reset the BI Publisher database user passwords (DEV_MDS, DEV_BIPLATFORM, or NNCENTRAL) by entering their original passwords that were specified during original database installation.

    ```
    SQL> alter user DEV_MDS identified by <original password>;

    User altered.
    ```

11. Logout as the Oracle system administrator (sysdba).

    ```
    SQL> exit;
    Disconnected from Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
    ```

12. Connect to BI Publisher database as one of the BI Publisher database users (DEV_MDS, DEV_BIPLATFORM, or NNCENTRAL) to ensure that the database is operational.

    For example:

    ```
    ./sqlplus DEV_MDS/<password>@AcmeBIPublis

    SQL*Plus: Release 11.2.0.1.0 Production on Tue Mar 29 10:43:17 2017
    ```

```
Copyright (c) 1982, 2009, Oracle.  All rights reserved.

Connected to:
Oracle Database 11g Release 11.2.0.1.0 - 64bit Production

SQL>
```

13. Logout as any one of the BI Publisher database users (DEV_MDS, DEV_BIPLATFORM, or NNCENTRAL).

```
SQL> exit;
Disconnected from Oracle Database 11g Release 11.2.0.1.0 - 64bit Production
```

14. Login again as the Oracle user and start BI Publisher on the WebLogic server.

> **Note:**
>
> If you have any problems starting BI Publisher, see the *Restart the WebLogic Server to Run Reports* section in the *Oracle Communications Report Manager Installation Guide* for more information.

```
nohup ./startWeblogic.sh &
```

15. Check the Weblogic server log to make sure that it was started successfully.

16. Switch to the nncentral user.

```
su nncentral
```

17. Change to the SDM server bin directory.

```
cd /home/nncentral/AcmePacket/NNC<version>/bin
```

18. Start the SDM server.

```
./startnnc.sh
```

19. Check the Reporting Service log to make sure that it was started successfully.

```
cd <OCSDM-INSTALL_DIRECTORY>/logs
grep "service started" ReportingService.log
2016-02-09 16:44:37,988 INFO
[com.acmepacket.ems.server.services.ReportingService] - Method:
[startService]
Thread: [ReportingService:25]  Msg:[...service started]
```

20. If you are running an SDM server cluster, repeat the previous steps for each cluster member node.