Oracle® Communications Services Gatekeeper

Integration Guide

Release 6.0

E55395-01

January 2015

ORACLE®

Oracle Communications Services Gatekeeper Integration Guide, Release 6.0

E55395-01

Contents

5 Integrating Services Gatekeeper with Service Controller

Preface

This book explains how to connect Oracle Communications Services Gatekeeper with a variety of different types of network nodes.

Audience

This document is intended for IT personnel who are integrating a Services Gatekeeper implementation into their network.

Documentation 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.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For related information, see the following Services Gatekeeper documents:

- *Oracle Communications Services Gatekeeper Getting Started Guide*
- *Oracle Communications Services Gatekeeper System Administrator's Guide*
- *Oracle Communications Services Gatekeeper Security Guide*

1

Understanding Services Gatekeeper Integration

This chapter provides an overview of the general issues you need to consider when connecting Oracle Communications Services Gatekeeper with the other network entities that your implementation requires.

Overview of Connecting Services Gatekeeper with Network Entities

Services Gatekeeper must integrate with a variety of network entities that provide support for the APIs and applications it serves. For example, databases store information that Services Gatekeeper uses; SMSCs serve and send short messages; the Oracle Communications Billing and Revenue Management product allows you to charge and rate for services. Each chapter in this book explains how to integrate Services Gatekeeper with a specific type of network entity:

- Integrating Services Gatekeeper with BRM

- Integrating Multi-tier Services Gatekeeper with Cloud Monitoring

- Integrating Services Gatekeeper with a PCRF

- Integrating Services Gatekeeper with Service Controller

2

Integrating Services Gatekeeper with BRM

This chapter explains how to integrate an Oracle Communications Services Gatekeeper implementation with the Oracle Communications Billing and Revenue Management (BRM). BRM is a product the you use to charge and rate for services. Integrating with BRM requires that you also obtain and configure the Oracle Communications Online Mediation Controller product.

Overview of Integrating Services Gatekeeper with Billing and Revenue Management

BRM is an end-to-end revenue management system for communications and media service providers. You use it to generate, capture, collect and analyze revenue for your applications.

This section assumes that you have:

- Used the instructions in *Services Gatekeeper Getting Started Guide* or *Services Gatekeeper Multi-tier Installation Guide* to install Services Gatekeeper and start the administration server.

- Followed the instructions in the *Services Gatekeeper Multi-tier Installation Guide* and installed the Oracle Communications Service Broker product which also contains the Online Mediation Controller product.

- Followed the instructions in *Oracle Communications Billing and Revenue Management Installation Guide* and installed and started the BRM product.

- That you know the IP addresses and system names of the servers that Services Gatekeeper and BRM are running on.

The tasks required to add BRM as a billing system to Services Gatekeeper include:

- Configuring Online Mediation Controller to Integrate with BRM

- Configuring Services Gatekeeper to Integrate with BRM

- Configuring BRM to Integrate with Services Gatekeeper

Configuring Online Mediation Controller to Integrate with BRM

To configure Online Mediation Controller to work with BRM:

1. Configure the SSU Diameter:

   - Add a relay route to the Services Gatekeeper system.

   - Add Services Gatekeeper as a Diameter Peer.

For instructions, see *Oracle Communications Online Mediation Controller Signaling Server Units Configuration Guide*.

2. Configure the SSU PCP to connect Service Broker to BRM.

   For instructions, see the section on configuring a PCP signaling server unit in *Oracle Communications Service Broker Signaling Server Units Configuration Guide*. Also see the section about setting up orchestrated charging mediation in *Oracle Communications Online Medication Controller Implementation Guide*.

3. Configure an IM-OCF PCP to connect Online Medication Controller to Service Broker.

   For information, see the section about setting up IM-OCF PCP in *Oracle Communications Service Broker Modules Configuration Guide*.

Configuring Services Gatekeeper to Integrate with BRM

This section explains how to configure Services Gatekeeper to communicate with the BRM implementation.

To configure Services Gatekeeper to communicate with BRM:

1. Open the Services Gatekeeper Administration Console or another MBean browser.

2. Configure the Diameter MBean:

   - **Origin-Host:** *Gatekeeper_IP_Address*

   - **Origin-Realm: ro.server.oracle.com**

   - **Service-Context-Id:** *Gatekeeper_context_address*

     For example:

     ```
     Service-Context-Id: SCP-NBI.208.01.S2F0@company.com
     ```

3. Configure an SLA by navigating to **Accounting Service**, then **ServiceLevelAgreementMBean**, then **setupCustomSlaXSDDefinition**.

4. Set **SlaType:** to **payment_diameter_avp**.

5. Set **FileContent:**. Copy the contents of *Middleware_home***/ocsg**_*release_ level*/**applications/wlng_nt_payment_px30.ear/plugin_px30_payment_ diameter.jar/xsd/paymentConifg.xsd** to this field.

6. Open this file for editing: *Middleware_home***/ocsg**_*release_level*/**applications/wlng_ nt_payment_px30.ear/plugin_px30_payment_ diameter.jar/xml/defaultavptemplate.xml**

7. Add a **Service-Identifier** AVP to **defaultavptemplate.xml**. For example:

   ```
   <avpTemplate>
   ...
   <avpValue avpName="Service-Identifier" defaultValue="3" />
   ...
   </avpTemplate>
   ```

8. Remove these AVPs from the **defaultavptemplate.xml** file:

   - **OCSG-application-Id**

   - **Event-Timestamp**

   - **OCSG_Reference-Code**

9. Save and close **defaultavptemplate.xml**.

10. In the Administration Console, navigate to *domain_home***/ocsg/AdminServer**, then **Accounting Service**, then **ServiceLevelAgreementMBean**, then **loadGlobalSlaByType**.

11. Set these fields in the MBean:

   - **SlaType: payment_diameter_avp**

   - **FileContent:** (copy the contents of the defaultavptemplate.xml file from Step 8 here.

   - **Service-Identifier:**

     - **Time(CC-TIME): 0**

     - **OCTET(CC-OCTEC): 4**

     - **User-Defined(CC-Specific-Units): 3**

Configuring BRM to Integrate with Services Gatekeeper

To configure BRM to communicate with Services Gatekeeper:

1. Start Pricing Center.

2. Set **Host:** to the Services Gatekeeper administration server hostname.

3. Set **Cm_port:** to the Services Gatekeeper administration server port number.

4. Set **Account tel:** to the Services Gatekeeper telephone number.

3

Integrating Multi-tier Services Gatekeeper with Cloud Monitoring

This chapter explains how to add multi-tier Oracle Communications Services Gatekeeper to Oracle Enterprise Manager Cloud Control (Enterprise Manager) monitoring control. Integrating single-tier Services Gatekeeper with Enterprise Manager is not supported.

About Integrating Enterprise Manager

You use Enterprise Manager to monitor applications and their individual servers and services. Enterprise Manager is an Oracle product that you purchase, install, and configure separately.

This chapter assumes that you are installing a production system and that:

- You have installed multi-tier Services Gatekeeper on its own system(s).

- You have installed Enterprise Manager on a its own system. For details, see *Oracle Enterprise Manager Installation Guide* and *Oracle Enterprise Advanced Installation and Configuration Guide* at the Oracle Enterprise Manager Cloud Control Documentation web site:

  http://docs.oracle.com/cd/E24628_01/index.htm

- You have installed the Enterprise Manager repository on its own system. For details, see *Oracle Enterprise Manager Installation Guide* and *Oracle Enterprise Advanced Installation and Configuration Guide* at the Oracle Enterprise Manager Cloud Control Documentation web site:

  http://docs.oracle.com/cd/E24628_01/index.htm

If you are not familiar with Oracle Enterprise Manager, see *Oracle Enterprise Manager Cloud Control Getting Started Guide* for an overview of the product and its features::

http://docs.oracle.com/cd/E24628_01/install.121/e39876/toc.htm

Using Enterprise Manager

You use Enterprise Manager to monitor your multi-tier Services Gatekeeper implementation components.

See "About Monitoring Services Gatekeeper Using Enterprise Manager" in *Services Gatekeeper System Administrator's Guide* for the list of Services Gatekeeper metrics that you can monitor using Enterprise Manager.

Understanding Plug-in Terminology

Enterprise Manager and Services Gatekeeper use different definitions of the term *plug-in*. The Services Gatekeeper documentation set and this chapter use *plug-in* to refer to a pre-packaged service that you can offer to your customers, such as SMS or terminal location. This chapter refers to the Services Gatekeeper plug-ins as simply *plug-ins*. An Enterprise Manager Cloud Control product plug-in is a collections of files that comprise a program that it monitors, such as Service Gatekeeper. This chapter refers to the files that Enterprise Manager uses to monitor Services Gatekeeper as the *Oracle Enterprise Manager Services Gatekeeper plug-in*.

About the Multi-tier Services Gatekeeper Components You Can Monitor

Enterprise Manager monitors these types of Services Gatekeeper targets within the Enterprise Manager **OCSG** (Services Gatekeeper) plug-in:

- Basic domains: Enterprise Manager monitors the administration server and its network tier and application tier as a single **AdminServer** unit.

- Typical domains: Enterprise Manager monitors all the servers on a typical Services Gatekeeper system as separate targets. If an administration server has two network tier servers, the Enterprise Manager Cloud Control Console displays a single **AdminServer** and two **WLNG_NT_1** and **WLNG_NT_2** servers as separate targets.

- The host system operating system: Enterprise Manager monitors each host system operating system as a separate target.

- The Enterprise Manager agent: Enterprise Manager puts an agent on each system it monitors. The agent ensures that each system is up and running.

- Plug-in services: Enterprise Manager monitors the plug-in services listed in Table 3–1.

Table 3–1   Services Gatekeeper Plug-in Services and Their Enterprise Manager Targets

Services Gatekeeper Plug-in Name	Enterprise Manager Target Name
Plugin_px21_call_notification_sip	OCSG_CallControl
Plugin_px21_third_party_call_inap	OCSG_CallControl
Plugin_px21_third_party_call_sip	OCSG_CallControl
Plugin_px30_audio_call_parlay_mpcc_cui	OCSG_CallControl
Plugin_px30_call_notification_parlay_mpcc	OCSG_CallControl
Plugin_px30_third_party_call_parlay_mpcc	OCSG_CallControl
Plugin_multimedia_messaging_mm7	OCSG_MMS
Plugin_px21_multimedia_messaging_email	OCSG_MMS
Plugin_px21_multimedia_messaging_mm7	OCSG_MMS
Plugin_px21_short_messaging_smpp	OCSG_SMS
Plugin_sms_smpp	OCSG_SMS
oracle.ocsg.native_ucp_sms	OCSG_SMS
Plugin_px21_presence_sip	OCSG_Presence
Plugin_px30_payment_diameter	OCSG_Payment
Plugin_px21_terminal_location_mlp	OCSG_Mobility

Table 3–1 (Cont.) Services Gatekeeper Plug-in Services and Their Enterprise Manager

Services Gatekeeper Plug-in Name	Enterprise Manager Target Name
Plugin_px21_terminal_status_map	OCSG_Mobility
Plugin_ews_push_message_pap	OCSG_PushMsg
Plugin_px30_device_capabilities_ldap	OCSG_Other
Plugin_ews_subscriber_profile_ldap	OCSG_Other

Adding Multi-tier Services Gatekeeper Support to Enterprise Manager

This section explains how to add Services Gatekeeper support to Enterprise Manager.

Installing the Services Gatekeeper Plug-in on Enterprise Manager

This section explains how to install the Enterprise Manager Services Gatekeeper plug-in on your Enterprise Manager system.

You must have the capability to transfer files between the Enterprise Manager system and the Services Gatekeeper system.

Installation Prerequisites

This chapter assumes that:

- You have installed Services Gatekeeper on an its own system.

- You have installed Enterprise Manager on its own system, and you have installed the Enterprise Manager repository on its own system. For details, see *Oracle Enterprise Manager Installation Guide* and *Oracle Enterprise Advanced Installation and Configuration Guide* here:

  http://docs.oracle.com/cd/E24628_01/index.htm

 You will need to provide the following information during installation:

- Enterprise Manager system details:
  - The server name
  - The server IP address
  - An operating system login user name and password
  - The Enterprise Manager home directory location
  - The Enterprise Manager Cloud Control Console URL
  - An Enterprise Manager Cloud Control Console user name and password

- Enterprise Management Repository system:
  - The server IP address
  - The server operating system login user name and password
  - The database password
  - The database SYS user name and password

- Services Gatekeeper system details. The Enterprise Manager documentation refers to this system as the *target host*:
  - The IP address

- An operating system login and password

- The WebLogic server user name and password

- The WebLogic server port to use

You install the Enterprise Manager Services Gatekeeper plug-in by using the Enterprise Manager Cloud Control Console. Enterprise Manager also has command-line options for the installation steps. For details about the command-line tools, see the Enterprise Manager Cloud Control documentation.

If you are new to Enterprise Manager and Oracle Management Service, see "Managing Plug-Ins" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for information about Enterprise Manager plug-ins and how to work with them.

Installing Multi-tier Services Gatekeeper On Enterprise Manager

To install the Enterprise Manager Services Gatekeeper plug-in:

1. On the Enterprise Manager system, start the Enterprise Manager console.

   See "Logging in to Enterprise Manager Cloud Control Console" for instructions.

2. Create a named credential with the user name, password, and running privileges as superuser on the Enterprise Manager system. This user should also have superuser permissions on the Services Gatekeeper target host.

3. Add the Services Gatekeeper system as a target host.

   See "Discovering, Promoting, and Adding Targets" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details.

4. Deploy an Enterprise Manager agent to the Services Gatekeeper target host.

   See "Discovering, Promoting, and Adding Targets" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details

5. On your Services Gatekeeper system, navigate to *Services_Gatekeeper_home***/ocsg/cloud-control**.

6. Copy the **.opar** file from your Services Gatekeeper system to the Enterprise Manager system. These instructions assume that you put it in **/tmp** on the Enterprise Manager system, but that location is not mandatory.

   The actual name of your **.opar** file varies depending on the release of Services Gatekeeper, but it looks similar to this: **12.1.0.6.0_oracle.emsysman.ocsg_2000_0.opar**

7. On your Enterprise Manager system, navigate to the Enterprise Manager installation home directory and use the **oms/bin/emcli** command to import the **.opar** file into your Enterprise Manager implementation. If a cluster contains more than one host, install it on the administration host:

```
cd enterprise_manager_home
oms/bin/emcli import_update -file="/file_location/your_cloud_file.opar"
-omslocal
```

   For example:

```
cd /home/oracle/em2
/oms/bin/emcli import_update -file="/tmp/12.1.0.6.0_oracle.emsysman.ocsg_ 2000_
0.opar" -omslocal
```

> **Note:** Do not import a given version of an **.opar** file more than once.

8. If the following error appears:

```
Error: Session expired. Run emcli login to establish a session.
```

Log in with this command:

```
oms/bin/emcli login -username=username
    (You are prompted for the password)
```

9. Deploy the Services Gatekeeper Enterprise Manager plug-in on the Enterprise Manager system (Oracle Management Service server).

See "Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime)" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details on deploying the Services Gatekeeper Enterprise Manager plug-in.

10. Deploy the Enterprise Manager agents on the Services Gatekeeper management agents.

If the system contains more than one Services Gatekeeper server, only deploy the plug-in to the administration server.

See "Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime)" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details on deploying the Services Gatekeeper Enterprise Manager plug-in.

11. Specify the Services Gatekeeper components to monitor as targets. See "Monitoring Multi-tier Services Gatekeeper Targets from Enterprise Manager Console" for a list of the Services Gatekeeper components that you can monitor as targets.

See "Discovering, Promoting and Adding Targets" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details on how to add components as targets.

12. Set up the Enterprise Manager Management Repository.

See *Oracle Enterprise Manager Cloud Control Installation and Configuration Guide* and *Enterprise Manager Cloud Control Administrator's Guide* for details about monitoring.

Next see "Monitoring Multi-tier Services Gatekeeper Targets from Enterprise Manager Console" for instructions on how to set up the Services Gatekeeper components to monitor.

Monitoring Multi-tier Services Gatekeeper Targets from Enterprise Manager Console

Each Services Gatekeeper implementation that you monitor has a root of **OCSG** in the **Target Navigation** window of the Enterprise Manager Cloud Control Console. The other Services Gatekeeper targets are subordinate to the root, and you can select them using the **Target Navigation** tools.

You can select the **OCSG** root, or any of the targets in the target menu. When you select a target, its status and any incidents caught during processing are displayed in the lower right pane.

Each target can also contain other targets. For example, a domain might contain a **MultimediaMesg** administration service server and several NT servers. A target is marked as available and running if at least one of a its plug-in services and one of its servers are running. Otherwise, the target is marked as unavailable.

See "Maintaining Enterprise Manager" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for details about what is displayed in the Enterprise Manager console.

About Using Enterprise Manager Monitoring Metrics

Enterprise Manager includes a comprehensive set of performance and system health metrics that you use to monitor the components of your Services Gatekeeper implementation. Each metric is a collection of statistics that Enterprise Manager monitors for each target. If the target has multiple servers, You can view Enterprise Manager statistics individual servers, or aggregated statistics for all servers. You can check Enterprise Manager Cloud Control Console as it gathers data, or you can direct it to generate metrics reports.

By default, the Services Gatekeeper metrics are aggregated. For example, all NT server metrics are aggregated, although you can also view them singly.

Enterprise Manager enables you to set metric thresholds that trigger metric alerts (events). The default alert levels are **Warning** and **Critical**. You can set these thresholds to meet your business requirements, and implement automatic corrective action to resolve the issues.

You will probably want to coordinate your monitoring thresholds with your SLA limits. For example you may want to be alerted with a **Warning** when a partner has exceeded 90% of a resource allocation, and a **Critical** message when they reach the limit. You could then alert them to that fact to avoid bill shock. It would also provide you with an opportunity to contact with an offer to sell the additional resources.

> **Caution:** The metric monitoring collection period is 5 minutes. It is important that you do not change this setting.

See "Overview of Enterprise Monitoring" in *Oracle Enterprise Manager Cloud Control Administrator's Guide* for an introduction to the metrics and metric templates.

You can also create your own metrics for your Services Gatekeeper implementation. See "Using Metric Extensions" for information and instructions about creating and modifying metrics to monitor.

After you configure the metrics for your business needs, you can specify them as *metric templates* and deploy them to the various components of your Services Gatekeeper implementation. This also enables you to quickly deploy the metrics as you add servers to your implementation.

For information about using metric templates, see "Monitoring: Advanced Setup" in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

4

Integrating Services Gatekeeper with a PCRF

This chapter explains how to add a Policy and Charging Rules Function (PCRF) network node to your Oracle Communications Services Gatekeeper implementation.

About Adding a PCRF to Services Gatekeeper

You use a PCRF to create and interpret quality of service (QoS) rules for the web services that Services Gatekeeper manages. You also need a Policy Enforcement Rules Function (PCEF) to enforce those rules. This chapter explains the general steps necessary to add a PCRF to your Services Gatekeeper implementation, using a Tekelec PCRF as an example. The instructions for adding other PCRFs are similar. These tasks are explained in the sections that follow:

- Prerequisites

- Start the Tekelec GUI and Reset Your Password

- Configure the PCRF Topology

- Configure Network Elements and a Services Gatekeeper Application

- Add a Policy Server

- Set the Policy Server's Log level

- Configure Services Gatekeeper to Communicate with the Tekelec PCRF

Adding a Tekelec PCRF to Services Gatekeeper

This section explains how to configure both the Tekelec PCRF and your Services Gatekeeper to communicate.

Prerequisites

This chapter assumes that you have:

- Installed Services Gatekeeper and started the domain servers.

- Acquired and started the Tekelec PCRF server.

- Acquired and know the IP address of a PCEF.

Start the Tekelec GUI and Reset Your Password

To add a Tekelec PCRF to Services Gatekeeper:

1. Open a web browser

2. Enter the IP address of the Tekelec PCRF.

   The Policy Management Initial Configuration Screen appears.

3. Check these checkboxes:

   - **Diameter 3GPP**

   - **Quotas Gx**

   - **Manage Policy Servers**

   - **Manage Policies**

   - **Manager is HA**

4. Click OK.

   The Tekelec Welcome page appears.

5. Enter the user name and password supplied by Tekelec and click **Login**.

   The password reset page appears.

6. Enter your current password and a new one.

7. Select **Change Password**.

   The Tekelec Policy Configuration Management Platform management console appears.

Configure the PCRF Topology

To configure the Tekelec topology:

1. From the Tekelec CMP management console, navigate to **Platform Setting**, then **Topology Setting**, then **All Clusters**, then **Add CMP Cluster**.

2. Enter your Services Gatekeeper server type in the **HW Type** field and IP address in the **OAM VIP** field.

   See the Tekelec documentation for the correct **HWType** setting.

3. See the Tekelec documentation for instructions on setting **Signaling VIP 1** field.

4. Click **Save**.

   The CMP server is restarted

5. Select **Topology Settings**, then **All Cluster**. then **Add MPE**.

6. Enter your Services Gatekeeper server type in the **HW Type** field and IP address i the **OAM VIP** field.

   See the Tekelec documentation for the correct **HWType** setting.

7. See the Tekelec documentation for instructions for setting the **Signaling VIP 1** field.

8. Navigate to **Platform Setting**, then **Topology Setting**, then **New Network Elements**.

9. Enter your Services Gatekeeper server type in the **HW Type** field and IP address i the **OAM VIP** field.

   See the Tekelec documentation for the correct **HWType** setting.

10. See the Tekelec documentation for instructions on setting the **Signaling VIP 1** field.

11. Click **Save**.

The MPE server is restarted.

Configure Network Elements and a Services Gatekeeper Application

To configure network elements, including setting the identify of the policy PCEF, Diameter server, and applications to use in your Services Gatekeeper/Tekelec PCRF implementation:

1. From the CMP management console, navigate to **Policy Server**, then **Network Elements**.

The **New Network Element** screen appears.

2. Enter a *pcef_name* for the new PCRF implementation in the **Name** field.

3. Enter the MPE server's IP address the **Host Name/ IP Address** field.

4. Select **GGSN** from the **Type** menu.

5. Select **Save**.

The PCEF element is created

6. Navigate to the **GGSN** tab.

The **Modify Network Element** screen appears.

7. Enter **oracle.com** in the **Diameter Realm** field

8. Enter **gx-ggsn** in the **Diameter Identity** field.

9. Select **Save**.

10. Navigate to **Policy Server**, then **Applications**.

The **New Applications** window appears.

11. Enter **Services_Gatekeeper** or another name for your Services Gatekeeper domain server in the **Name** field.

12. Enter an informal description in the **Description** field.

13. Enter the Services Gatekeeper IP address in the **Connection IP Address(es)** field.

14. Enter an informal name for the Diameter identity.

15. Select **Save**.

Your Services Gatekeeper implementation is added as an application.

Add a Policy Server

To configure a policy server:

1. Tekelec CMP management console, navigate to **Policy Server,** then **Configurations**.

The **New Policy Server** window appears.

2. Select **MPE** from the Associated Cluster Name menu.

3. Select **Tekelec** from the **Type** menu.

4. Click **Save**.

The new MPE Policy Server is created.

Configure the MPE Policy Server

To configure the MPE policy server:

1. In the CMP management console, navigate to **Policy Server**, then **Configurations**, then select the **Policy Server** tab.

2. Enter the name for your Services Gatekeeper application in the **Applications** field. You used the name **Services_Gatekeeper** in "Configure Network Elements and a Services Gatekeeper Application".

3. Enter **PCEF**, in the **Network Elements** field.

4. In the **Subscriber Indexing** field, set **IMSI: Index by IMSI** to **true**.

5. Enter your Diameter server port number in the **Diameter Port** field. **6868** is the default.

6. Enter **oracle.com** in the **Diameter Realm** field.

7. Enter **oracle** in the **Diameter Identity** field.

8. Click **Save**.

Set the Policy Server's Log level

To set the policy server's log level:

1. In the CMP management console, navigate **Policy Server**, then **Configurations**, then select the **Logs** tab.

2. Select **Info** from the **Trace Log Level** menu.

3. Click **Save**.

Configure Services Gatekeeper to Communicate with the Tekelec PCRF

To configure Services Gatekeeper to communicate with the Tekelec PCRF:

1. Open the Services Gatekeeper Administration Console.

2. Navigate to **wlng_nt_qos#***release_level*, then **QoSMBean**, then **DestinationAddresses**.

3. Enter the IP address of your Tekelec PCRF in the **DestinationAddresses**: field.

4. Click Save.

5. Navigate to **OoSMbean**, then **DestinationRealm**.

6. Enter the **oracle.com** in the **DestinationRealm** field.

7. Click Save.

Configure the PCRF QoS Rules

Now that you have configured a PCRF to communicate with Services Gatekeeper, you need to configure the QoS rules that define your implementation's QoS products. That discussion is beyond the scope of the Services Gatekeeper documentation. See your PCRF documentation for details.

5

Integrating Services Gatekeeper with Service Controller

This chapter lists the Oracle Communications Services Gatekeeper communication services that can take advantage of Oracle Communications Service Controller features.

About Integrating Services Gatekeeper with Service Controller

You can integrate Services Gatekeeper with Oracle Communications Converged Application Server, Service Controller edition if your implementation requires service orchestration and protocol mediation capabilities.

A Service Controller-Service Gatekeeper integration must communicate using SIP traffic, and Services Gatekeeper must then translate the SIP traffic into SS7 format. Consequently, these are the network-facing communication services that can take advantage of the integration:

- Parlay X 2.1 Audio Call/SIP
- Parlay X 2.1 Call Notification/SIP
- Parlay X 2.1 Presence/SIP
- Parlay X 2.1 Third Party Call/SIP
- RESTful Third party Call
- RESTful Call Notification
- RESTful Audio Call
- RESTful Presence

For details on these communication services, see the *Services Gatekeeper Communication Service Reference Guide* and "Creating Applications Using the RESTful Interfaces" *Services Gatekeeper Application Developer's Guide*.