Oracle® Communications Services Gatekeeper

Release Notes

Release 4.1

January 2009

ORACLE

Oracle Communication Services Gatekeeper Release Notes, Release 4.1

Contents

1. New Features

2. Backwards Compatibility

3. Gatekeeper 4.1 Known and Resolved Issues

CHAPTER 1

New Features

Welcome to Oracle Communications Services Gatekeeper™ 4.1. As the leading Telecom Service Access Gateway, Gatekeeper integrates telecom network technologies with SOAP Web Services, RESTful Web Services and SOA to provide a reliable framework for developing and deploying highly available, scalable, and secure telecommunications applications and features. Oracle Communications Services Gatekeeper's seamless integration of disparate, heterogeneous platforms and applications enables your network to leverage existing software investments and share the carrier-class services and data that are crucial to building next-generation telecommunication applications.

This chapter describes at a high level what new features in Gatekeeper have been created to support the ongoing evolution of the platform.

Evolving the Platform

Versions 3.0 and 4.0 marked a substantial change to the basic architecture of Oracle Communications Services Gatekeeper. Version 4.1 builds on that change, preparing the way for future developments.

Built on WebLogic Server 10.3

In version 4.1, Oracle Communications Services Gatekeeper has been moved to Oracle WebLogic Server 10.3. This has multiple benefits for the Oracle Communications Services Gatekeeper platform, including:

- Improved scalability and performance

- An improved Administration Console with a new look and feel, on-demand deployment capability, performance enhancements, improved accessibility, and improved browser support
- Support for HTTP Publish-Subscribe Server
- Support for Sun JDK 1.6

For more information, see the "What's New" section of the WebLogic Server 10.3's release notes at http://download.oracle.com/docs/cd/E12840_01/wls/docs103/notes/new.html

Tight Integration with Oracle Communications Converged Application Server for SIP Connectivity

Oracle Communications Converged Application Server (previously WebLogic SIP Server) is now co-located with Oracle Communications Services Gatekeeper. This offers several benefits:

- Performance: For Service Enablers using the SIP protocol, co-location provides significant performance enhancements.
- Simplified configuration: Because the Converged Application Server is pre-integrated and co-located with Oracle Communications Services Gatekeeper's Network Tier servers, there is no longer a need for a multi-domain setup and the configuration of integration software. The Oracle Communications Services Gatekeeper's installer automatically installs the software and the Configuration Wizard handles the domain setup and deployment.
- Single console: A single Oracle Communications Services Gatekeeper Administration Console can be used to control and configure both Oracle Communications Services Gatekeeper and the Converged Application Server.
- Integrated servlet: Tight integration means that the SIP servlet is now encapsulated in the communication service plug-in.

  Note: All out-of-the-box Service Enablers that provide SIP connectivity have been updated to use the new deployment model.

For more information on the Converged Application Server in the context of Oracle Communications Converged Application Server, see the *System Administrator's Guide*, another document in this set.

Pre-integrated with Oracle Communications Billing and Revenue Management

Oracle Communications Services Gatekeeper integrates with Oracle Communication Billing and Revenue Management (OCBRM) for billing. Using DIAMETER, Oracle Communications Services Gatekeeper integrates with the billing platform using a set of three integration points.

- The Parlay X 2.1 Payment/DIAMETER communication service allows applications to reserve funds from subscriber accounts and charge them directly on-line using the DIAMETER Ro interface. Pre-integration with Oracle Communications Billing and Revenue Management is provided, although any billing system that supports DIAMETER Ro can be used.
- Any request flowing through Oracle Communications Services Gatekeeper can be subject to credit control checks. Using criteria based both on the request data and other configurable data, these interceptors pass requests to the billing server using the DIAMETER Ro interface. The billing server verifies that the subscriber or application has enough credit to allow the request. Credit control checks can be performed both for application-initiated and network-triggered requests. All, or a configurable subset of the requests, can be subject to these credit control checks. Pre-integration with Oracle Communications Billing and Revenue Management is provided, although any billing system that supports DIAMETER Ro can be used.
- Offline billing is supported using the CDR to Diameter Service. Charging Data Records (CDRs) generated by Oracle Communications Services Gatekeeper are passed on to the billing server using the DIAMETER Rf interface. Pre-integration with Oracle Communications Billing and Revenue Management is provided, although any billing system that supports DIAMETER Rf can be used.

For more information on Oracle Communications Billing and Revenue Management, see the E-Delivery site: http://edelivery.oracle.com/. A password is required.

Enhanced SLA Structure and Enforcement

Significant changes have been made to increase the flexibility and utility of SLA definition, enforcement, and provisioning.

Service Types

A new enforcement category, Service Type, has been introduced. In previous versions, request rates and quotas could be defined and enforced only on the method level, which offered great flexibility, but sometimes made SLA structures unnecessarily complex. Using service types, the

service contract can be defined at a less granular level, when that is appropriate for the use case. A service type groups a set of Service Enablers based on functionality. For example, the Service Enablers for both Parlay X 2.1 and 3.0 Third Party Call are grouped into the service type ThirdPartyCall.

SLA Types

SLAs are now divided into two large groups: system SLAs and custom SLAs. System SLAs are those that cover commonly found aspects of Oracle Communications Services Gatekeeper contractual relationships. Custom SLAs are used to add enforcement mechanisms not covered by the system SLA types.

Custom SLAs can be created to cover a variety of operator use cases. Oracle Communications Services Gatekeeper provides the infrastructure to define, enforce and provision custom SLAs while the XSD and enforcement of the SLA are controlled by the operator. The enforcement logic has access to the data in the request being enforced, the data in the SLA, and other related data about the request, such as the application ID and service provider ID. Once the enforcement logic is deployed and the XSD for the custom SLA is loaded, an SLA type for the SLA is defined and these SLAs can be provisioned just like system SLAs.

SLAs for Geo-Redundancy

With version 4.1, Oracle Communications Services Gatekeeper allows geo-redundant site pairs to share a broad range of configuration data between sites as well as the budget information supported in version 4.0. Previously an element in the SLA, `<enforceAcrossSites>`, indicated that included information was to be synchronized across sites. Now separate SLA types exist to separate data that should be geo-synchronized from data that needs to be local to a particular site.

Provisioning

SLA provisioning has been simplified with new management methods. Instead of having individual methods for the management of each SLA type, the type is simply passed in as a parameter. Also new interfaces supporting this change have been added to the operator interface offered by the Partner Relationship Management module, allowing PRM to make changes that can be propagated throughout the domain, or, in the case of a geo-redundancy, across site pairs.

For more information on SLAs, see *Managing Accounts and SLAs*, a separate document in this set.

New Service Facades for Exposure

Version 4.0 of Services Gatekeeper provided service providers and applications access using standards-based SOAP Web Services. Version 4.1 adds additional modes of access, and introduces the concept of Service Facades. A Service Facade defines the type of access that an application uses to interact with Oracle Communications Services Gatekeeper. These facades include:

- Traditional SOAP-based Web Services. Version 4.1 supports all of the interfaces offered in 4.0 and adds a Parlay X 3.0 Payment interface, a Parlay X 2. 1 Presence Supplier interface, and a mobile-originated Binary SMS Extended Web Services functionality.
- RESTful Web Services. Applications can now access the capabilities of communication services through RESTful APIs. These APIs can be used to smoothly integrate telecommunication features into Web 2.0 Rich Internet Application environments.
- Native protocols. Many carriers already have an ecosystem of existing applications that use traditional network protocols. For these operators Oracle Communications Services Gatekeeper offers MM7 and SMPP Native interfaces. Oracle Communications Services Gatekeeper, acting as a server, exposes these native interfaces to applications, and then, acting as an application, passes the requests on to the network element. This model allows these applications to continue to exist unchanged while allowing the operator to leverage the system-level features offered by Oracle Communications Services Gatekeeper, including the generation of CDRs, EDRs, and alarms, the enforcement of SLAs and so forth.
- SOA. From the point of view of the application, the SOA facade exposes the same interfaces as the SOAP based Web Service facade. But these interfaces are exposed using the Oracle Service Bus, allowing the operator to access the additional functionality of SOA. Operators can, among other things, use OSB to define routing logic and parameter substitution, smoothly integrating Oracle Communications Services Gatekeeper into the operator's SOA environment. The SOA service facades are deployed in Oracle Service Bus (OSB) itself, which replaces the Oracle Communications Services Gatekeeper Access Tier. for more information on Oracle Service Bus, see http://download.oracle.com/docs/cd/E13159_01/osb/docs10gr3/index.html

Any combination of Service Facades may be deployed in a standard Oracle Communications Services Gatekeeper deployment.

Note: In a multi-cluster, single domain deployment, only one cluster may deploy SOA or RESTful interfaces.

For more information on service facades, see "Developing Applications" in *Concepts and Architectural Overview*, a separate document in this set.

Enhanced Plug-in Routing

Earlier versions of Oracle Communications Services Gatekeeper made routing decisions based exclusively on the destination address. This version allows routing decisions to be made on multiple characteristics including:

- The Service Provider ID and the Application ID
- The method being invoked
- Any parameter, or combination of parameters, in the request
- Tunneled parameters

The data is filtered by routing logic, using combinations of logical AND, OR, and NOT operations. The routing logic is expressed in XML, and is specified per plug-in instance.

For more information on plug-in routing, see "Managing and Configuring the Plug-in Manager" in *System Adminstrator's Guide*, a separate document in this set.

Robust Tier Routing

The Tier Routing Manager operates on network-triggered requests and routes these request to the appropriate service facade type. For more information on the Tier Routing Manager, see "Managing and Configuring the Tier Routing Manager" in *System Adminstrator's Guide*, a separate document in this set.

PRM

PRM has been updated to use the new SLA provisioning methods. For more information, see "Operator Service" in *Integration Guidelines For Partner Relationship Management*, a separate document in this set.

New Domain Templates

The Domain Configuration Templates have been updated to support the new service facades: SOAP, RESTful, and SOA. For more information, see "Configuring the Domain for Oracle Communications Services Gatekeeper"

New and Updated Communication Services

Parlay X 3.0 Payment/DIAMETER

A Parlay X 3.0 Payment communication service that connects to DIAMETER has been added to support online charging.

Parlay X 2.1 Presence/SIP

The Parlay X 2.1 Presence/SIP communication service has added Presence Supplier functionality as well as the Presence Consumer functionality of version 4.0

Native SMPP

To support existing SMPP-based applications in the operator's eco-system, a native SMPP communication service has been added. Towards the application it acts as a server and towards the network it acts as an application.

Native MM7

To support existing MM7-based applications in the operator's ecosystem, a native MM7 communication service has been added. Towards the application it acts as a server and towards the network it acts as an application.

Extended Web Services Binary SMS

Extended Web Services Binary SMS/SMPP has been enhanced with support for network-triggered, mobile originated, SMS.

RESTful Interfaces

Oracle Communications Services Gatekeeper's communication services can now be accessed using RESTful APIs.

Platform Development Studio

The Platform Development Studio has been expanded, including:

- SOAP-to-SOAP communication services can be generated through the Administration Console
- General communication service development has been streamlined and enhanced
- The Platform Test Environment now has a budget monitor, which is capable of graphing real-time budget usage
- Templates for the automatic generation of skeletons and stubs for SIP-type communication services have been added
- RESTful Web Services facades can be generated in addition to SOAP Web Services facades

Supported Interfaces

Gatekeeper 4.1 has support for a number of application-facing interfaces. The following communication services (application-facing interfaces with related network plugins) are included in this release, including three call control services built on the Parlay X 3.0 standards, which allow multiple functionalities to interact within the same call session. They include:

- Parlay X 3.0 Audio Call connecting to Parlay 3.3
- Parlay X 3.0 Third Party Call connecting to Parlay 3.3
- Parlay X 3.0 Call Notification connecting to Parlay 3.3
- Parlay X 2.1 Third Party Call connecting to INAP and SIP
- Parlay X 2.1 Call Notification connecting to SIP
- Parlay X 2.1 SMS connecting to SMPP 3.4
- Extended Web Services Binary SMS connecting to SMPP 3.4
- Parlay X 2.1 MMS connecting to MM7 v 5.5.0
- Parlay X 3.0 Payment connecting to DIAMETER
- Parlay X 2.1 Terminal Location connecting to MLP3.0/3.2
- Parlay X 2.1 Presence connecting to SIP
- Extended Web Services WAP Push connecting to PAP 2.0
- Extended Web Services Subscriber Profile connecting to LDAPv3

- SMPP 3.4 connecting to SMPP 3.4
- MM7 v 5.3.0 connecting to MM7 v 5.3.0
- RESTful Third Party Call connecting to SIP
- RESTful Call Notification connecting to SIP
- RESTful SMS connecting to SMPP 3.4
- RESTful MMS connecting to MM7 v 5.5.0
- RESTful Payment connecting to DIAMETER
- RESTful Terminal Location connecting to MLP3.0/3.2
- RESTful Presence connecting to SIP
- RESTful WAP Push connecting to PAP 2.0
- RESTful Subscriber Profile connecting to LDAPv3

Supported Configurations

The supported configurations have not changed since Oracle Communications Services Gatekeeper 4.0. For a complete listing, see the Technical Specifications chapter in the *Installation Guide*.

CHAPTER 2

Backwards Compatibility

This section covers backwards compatibility between Weblogic Network Gatekeeper 4.0 and Oracle Communication Services Gateway 4.1. The following areas are discussed:

- Platform Upgrades
- Management Operations
- Database
- Service Level Agreements

Platform Upgrades

Upgrades from Network Gatekeeper 4.0 to Gatekeeper 4.1 are supported. The upgrade process can be managed using the rolling upgrade mechanism unless your installation uses SIP, SMPP, or the new RESTful facade, in which case a restart is necessary. Scripts and tools to facilitate upgrade and migration of data are provided.

Management Operations

Some account management operations have changed to accommodate the new SLA Types. Older methods continue to work, but are deprecated. Some plugin routing operations have changed to accommodate the new tier routing mechanism. Full documentation is available in *Managing Accounts and SLAs* and *Integration Guidelines for Partner Relationship Management*, separate documents in this set.

Database

Database schemas have been changed and migration scripts are provided for upgrades.

Service Level Agreements

The Service Level Agreement mechanism has been expanded. Old SLAs will continue to work, but will not be synchronized across geographically remote sites regardless of the setting of the `<enforceAcrossSites>` tag, which has been deprecated. For more information on the changes to SLAs, see "Enhanced SLA Structure and Enforcement" on page 1-3.

As a result of these changes, there are several account management operations that have been changed, and earlier operations have been deprecated, both at the console (MBean) level and at the PRM Operator Service level. The deprecated operations in the console include:

- loadApplicationGroupSla
- loadApplicationGroupFromUrl
- retrieveApplicationGroupSla
- loadServiceProviderGroupSla
- loadServiceProviderGroupSlaFromUrl
- retrieveServiceProviderGroupSla
- loadGlobalNodeSla
- retrieveGlobalNodeSla
- loadServiceProviderGroupNodeSla
- loadServiceProviderGroupNodeSlaFromUrl
- retrieveServiceProviderGroupNodeSla
- loadSubscriberSla
- loadSubscriberSlaFromUrl
- retrieveSubscriberSLA

For more information on these changes, see "Managing SLAs" in *Managing Accounts and SLAs*, a separate document in this set.

The deprecated operations in the Operator Service interface of the PRM include:

- createAppGroup
- updateAppGroup
- createSpGroup
- updateSpGroup

For more information on these changes, see "Operator Service" in *Integration Guidelines for Partner Relationship Management*, a separate document in this set.

Gatekeeper 4.1 Known and Resolved Issues

Resolved Issues in Gatekeeper 4.1

.

Change Request Number	Description and Workaround or Solution	Found In	Fixed In
CR372355	Non-ASCII values for sendName in SMS and Binary SMS sendSMS result in garbled data. Values for this parameter must be ASCII per the SMPP standard.	4.0	4.1
CR372834	The MLP Simulator in Platform Test Environment will parse longitude/latitude incorrectly when the locale is not English. Switch locale to English	4.0	4.1
CR365666	Installing the Windows version using the installer does not work if the installer file is in the root directory of the disk. Remove the installer file from root and place in a sub-folder.	4.0	Closed

Change Request Number	Description and Workaround or Solution	Found In	Fixed In
CR366737	Some Gatekeeper DB tables specify primary keys and/or indexes that exceed the maximum key length for MySQL with MyISAM table type and UTF-8 character type. Either: 1. If you are using the MyISAM engine, set the character type to latin1 or 2. Use the InnoDB engine with UTF-8 or latin1 character set	4.0	4.1
CR370718	Return values from methods on the Store are not size limited. This can cause out-of-memory errors if the dataset is very large. Make sure your queries don't fetch the entire key/entry/value set from stores	4.0	4.1
CR372233	Warnings are thrown even when the silent installer is run successfully. These warnings have no impact on functionality.	4.0	4.1
CR372323	An IllegalArgumentException can be thrown when retrieving MMS message details in the Platform Test Environment. This usually does not affect the outcome of the operation.	4.0	4.1
CR372242	Gatekeeper can create new connections to the database when all the connections in the pool are in use. This can cause lock contention. Make sure that the database is configured with an adequate value for `MaximumCapacity`.	4.0	4.1
CR372847	The Statistics Service createWeeklyReport operation fails to retrieve a value which the report requires, which causes the operation to fail.	4.0	4.1

Change Request Number	Description and Workaround or Solution	Found In	Fixed In
CR346962	If the address of the MLP server is changed using OAM, the plug-in does not try to connect to the new server immediately. Instead it waits for the heartbeat interval before trying to connect.	3.0MP1	4.1
CR310647	During startup, there is a warning that no appenders can be found for loggers. The messages occur in the brief period of time when classes try to log messages before log4j has been initialized. They do not indicate a problem.	3.0	Closed

Known Issues in Gatekeeper 4.1

Change Request Number	Description and Workaround or Solution	Found In	Fixed In
CR384334	If you stop one AT server and one NT server in a multi-cluster domain and then restart only the AT server, application-initiated requests sent to that server may result in the following error with the message: “Failed to invoke end component <component name>”. In the reverse case, network-triggered requests may fail. Dependent on Oracle WebLogic Server CR384639. Make sure you start both servers. Contact Oracle support for a patch on this issue.	4.1	

CR384442	On the first start-up after domain configuration, if 2 or more NT servers are started at the same time, the servers may throw LDAP exception. An equivalent failure may occur on deploying applications. Restart the servers. If the problem persists, start one server first, and then the others Retry deploying the application. If the problem persists, redeploy the application when the servers are not running.	4.1
CR384688	Before geo-redundancy is set up, you may sometimes get null pointer exception in geo-storage module. This is benign and may be ignored.	4.1
CR384693	Setting `StatisticsServiceMbean::StoreInterval` to 0 can produce negative data in the transactions field of the `slee_statistics_data` table. Don't set StoreInterval to 0	4.1
CR384696	When OCSG is first used, the database is initialized. If two NT servers are started up at the same time, they may both try to initialize the database, causing a Service Deployment Exception and one server failing to start up. Make sure the servers are started one at a time. Restart the failed server.	4.1
CR384729	Some Diameter requests may be dropped during patching, redeployment, or upgrade of the CDR to Diameter module. Check the database for the time period during which the transition took place. All CDRs are stored in the database.	4.1

CR384771	If the credit control interceptor fails to connect to the Diameter server, the `isConnected` attribute will show incorrect state. Run traffic to check whether the interceptor is connected.	4.1
CR384818	The Native SMPP Communication Service does not support hitless upgrades. Upgrades cannot be performed without traffic service interruption. Perform a rolling upgrade instead.	4.1
CR384822	The Parlay X 2.1Short Messaging/SMPP plug-in does not support in-production upgrade after upgrading from 4.0. Before you do a rolling upgrade to the servers, undeploy the EAR file for this communication service. After all upgrades are complete, redeploy the EAR. This does not affect fresh installations of 4.1. **Note:** A mandatory patch will be released to correct this error. Please contact your Oracle service representative about acquiring this patch when it comes out.	4.1
CR384839	The Plug-in Manager reports that plugin_sms_smpp state is connected even when it is not. Use the ActiveStatus attribute of the SMPP MBean to check connection status	4.1
CR384863	When running the Legacy SMPP communication service, you may receive the following exception from your NT servers. `ERROR com.bea.wlcp.wlng.legacy.smpp.connector.SmppChannelProcessor - Could not find request for received response` This exception can be ignored.	4.1

CR384497	Due to incompatible class changes to the stored blob data, old application data (notifications, etc.) in SIP call notification and presence plug-ins will NOT be usable after the upgrade. Exceptions will be thrown during the upgrade when the old application data is accessed. Contact Oracle support for migration scripts.	4.1
CR384759	There is an error in the data migration scripts that causes the old SP SLA not to be changed. Necessary script updates can be found in "Upgrading Oracle Communications Services Gatekeeper" in *Installation Guide*, a separate document in this set.	4.1
CR371114	PRM service provider users and operator users can not be given access to a restricted set of JMX interfaces exposed by Oracle Communications Services Gatekeeper. Dependent on Oracle WebLogic Server CR 382906.	4.1
CR380863	The SOAP to SOAP generation does not support all WSDLs. The WSDL defining the application-facing interface must adhere to the following: • Attribute name in <wsdl:service> must include the suffix Service. • Attribute name in <wsdl:port> must be the same as the name attribute in • <wsdl:service>, excluding the suffix Service. Dependent on Oracle WebLogic Server CR 384278.	4.1
CR382790	The Native SMPP communication service does not actively disconnect applications if the SMSC connection is down. The communication service sends an OK response to enqure link requests in this case.	4.1