Oracle® Communications Services Gatekeeper

System Backup and Restore Guide

Release 5.1

E37530-01

June 2013

ORACLE®

Oracle Communications Services Gatekeeper System Backup and Restore Guide, Release 5.1

E37530-01

Contents

A Oracle Communications Services Gatekeeper Tables

Preface

This document explains how to back up and restore the modules in an Oracle Communications Services Gatekeeper domain.

Audience

This book is intended for system administrators and support engineers responsible for maintaining an Oracle Communications Services Gatekeeper system.

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 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 more information, see the following documents in the Services Gatekeeper set:

- *Oracle Communications Services Gatekeeper Accounts and SLAs Guide*
- *Oracle Communications Services Gatekeeper Alarm Handling Guide*
- *Oracle Communications Services Gatekeeper Application Developer's Guide*
- *Oracle Communications Services Gatekeeper Communication Service Guide*
- *Oracle Communications Services Gatekeeper Concepts Guide*
- *Oracle Communications Services Gatekeeper Installation Guide*
- *Oracle Communications Services Gatekeeper Licensing Guide*
- *Oracle Communications Services Gatekeeper Partner Relationship Management Guide*
- *Oracle Communications Services Gatekeeper Platform Development Studio Developer's Guide*
- *Oracle Communications Services Gatekeeper Platform Test Environment Guide*
- *Oracle Communications Services Gatekeeper RESTful Application Developer's Guide*

- *Oracle Communications Services Gatekeeper SDK User's Guide*
- *Oracle Communications Services Gatekeeper Statement of Compliance*
- *Oracle Communications Services Gatekeeper System Administrator's Guide*

1 Introduction

A variety of events can lead to the failure of a server instance. Often one failure condition leads to another. Loss of power, hardware malfunction, operating system crashes, network partitions, or unexpected application behavior may each contribute to the failure of a server instance.

Oracle Communications Services Gatekeeper uses a clustered architecture as the basis for minimizing the impact of failure events. However, even in a clustered environment it is important to prepare for a sound recovery process in the event that an individual server or server machine fails.

This chapter summarizes Services Gatekeeper failure prevention and recovery features and describes the configuration artifacts that are required to restore different portions of a Services Gatekeeper domain. The remaining sections in this guide describe how to back up Services Gatekeeper configuration artifacts and how to use those artifacts to restore the system in the event of a server failure.

Failure Prevention and Automatic Recovery Features

Services Gatekeeper, and the underlying Oracle Fusion Middleware WebLogic Server platform, provide many features that protect against server failures. In a production system, all available features should be used to ensure uninterrupted service.

Overload Alarms

Services Gatekeeper's underlying Oracle Fusion Middleware WebLogic Server platform detects increases in system load that can affect deployed application performance and stability. Oracle Fusion Middleware WebLogic Server also allows administrators to configure failure prevention actions that occur automatically at predefined load thresholds. Automatic overload protection helps avoid failures that result from unanticipated levels of application traffic or resource utilization as indicated by:

Each backward-compatible communication service in Services Gatekeeper uses a pair of attributes, OverloadPercentage and SevereOverloadPercentage, that define the amount of load on the software module required to trigger an overload alarm. Always monitor for these alarms and perform system throttling as necessary to avoid failures that could result from unanticipated levels of application traffic or resource utilization.

- A workload manager's capacity being exceeded
- The HTTP session count increasing to a predefined threshold value
- Impending out-of-memory conditions

For more information on avoiding and managing performance problems see "Avoiding and Managing Overload" in *Oracle Fusion Middleware Configuring Server Environments for Oracle WebLogic Server 11g* at:

http://download.oracle.com/docs/cd/E15523_01/web.1111/e13701/overload.htm

Redundancy and Failover for Clustered Services

Using multiple Access tier and Network tier servers in dedicated clusters increases the reliability and availability of applications.

Access tier clusters maintain no stateful information about applications, so the failure of a server does not result in any data loss.

Services Gatekeeper also performs automated failover for servers within the Network tier. Production installations must use the tiered configuration to protect against individual server failures. See "Redundancy, Load Balancing, and High Availability" in *Oracle Communications Services Gatekeeper Concepts Guide* for more information.

Automatic Restart for Managed Servers

Oracle Fusion Middleware WebLogic Server self-health monitoring features improve the reliability and availability of server instances in a domain. Selected subsystems within each server instance monitor their health status based on criteria specific to the subsystem. (For example, the JMS subsystem monitors the condition of the JMS thread pool while the core server subsystem monitors default and user-defined execute queue statistics.) If an individual subsystem determines that it can no longer operate in a consistent and reliable manner, it registers its health state as FAILED with the host server.

Each Oracle Fusion Middleware WebLogic Server instance, in turn, checks the health state of its registered subsystems to determine its overall viability. If one or more of its critical subsystems have reached the FAILED state, the server instance marks its own health state FAILED to indicate that it cannot reliably host an application.

When used in combination with Node Manager, server self-health monitoring enables automatically rebooting servers that have failed. This improves the overall reliability of a domain, and requires no direct intervention from an administrator. For more information on how to set up Node Manager and use it to control servers, see *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server* at:

http://download.oracle.com/docs/cd/E15523_01/web.1111/e13740/toc.htm

Managed Server Independence Mode

Managed Servers maintain a local copy of the domain configuration. When a Managed Server starts, it tries to contact the Administration Server to retrieve any changes to the domain configuration that were made since the Managed Server was last shut down. If a Managed Server cannot connect to the Administration Server during startup, it can use its locally-cached configuration information , which describes the configuration that was current at the time of the Managed Server's most recent shutdown. A Managed Server that starts up without contacting its Administration Server to check for configuration updates is running in Managed Server Independence (MSI) mode. By default, MSI mode is enabled. For information on replicating domain config files, see "Replicate domain config files for Managed Server independence" in *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* at:

http://download.oracle.com/docs/cd/E15523_
01/apirefs.1111/e13952/core/index.html

Automatic Migration of Failed Managed Servers

With Linux or UNIX operating systems, you can use Oracle Fusion Middleware WebLogic Server's server migration feature to start a candidate (backup) server automatically if a Network tier server's machine fails or becomes partitioned from the network. The server migration feature uses Node Manager, in conjunction with the **wlsifconfig.sh** script, to boot candidate servers automatically using a floating IP address. Candidate servers are booted only if the primary server hosting a Network tier instance becomes unreachable. For more information about using the server migration feature, see "High Availability for WebLogic Server" in *Oracle Fusion Middleware High Availability Guide* at:

http://download.oracle.com/docs/cd/E15523_01/core.1111/e10106/toc.htm

Geographic Redundancy for Regional Site Failures

In addition to server-level redundancy and failover capabilities, Services Gatekeeper enables configuration of peer sites to protect against catastrophic failures, such as power outages, that can affect an entire domain. It is possible to set up failover from one geographical site to another, avoiding complete service outages. See "Geographic Redundancy" in *Oracle Communications Services Gatekeeper Concepts Guide* for more information.

Overview of Configuration Artifacts

A Services Gatekeeper deployment utilizes two basic categories of configuration information: domain-level configuration, and database configuration. The domain-level configuration consists of the artifacts used by the underlying Oracle Fusion Middleware WebLogic Server platform to configure the behavior of managed servers, clusters, security, and other resources deployed to clusters and servers within the domain. The primary domain-level configuration artifact is the **config.xml** file, stored in the *Domain_Home*/**config** directory. The **config.xml** file generally references additional configuration files beneath the **config** directory to configure additional domain resources such as JDBC and JMS.

In addition to the basic domain-level configuration of the Oracle Fusion Middleware WebLogic Server platform, Services Gatekeeper stores some configuration for its core services in database tables. This includes the routing configuration for backward-compatible communication services and PRM integration data. The database tables are shared across clustered instances of Services Gatekeeper server instances. The database must be backed up at regular intervals to protect against data loss or corruption. An Oracle Real Application Cluster (RAC) deployment is also required for production installations, to provide redundancy and failover for the database configuration.

Both domain-level configuration backups and database backups may be required at different times to restore servers fully or to migrate server instances to new server hardware in a Services Gatekeeper installation.

Database Backup

Backing up the underlying database on a regular basis is an essential part of maintaining a Services Gatekeeper implementation. However that task is beyond the scope of this documentation. See your the Oracle database documentation for details on how to perform database backups.

Summary of Common Backup and Restoration Tasks

Maintaining system integrity requires that you make use of existing high availability and failover features, perform regular backups of configuration artifacts, and understand how to restore server instances or migrate servers onto viable hardware. These common tasks are summarized below.

- **Back up Oracle 10g, 11g, or MySQL database**.

  See your database backup and recovery documentation for details.

- **Enable Oracle Fusion Middleware WebLogic Server platform reliability and recovery features.**

  For a description of how to avoid and manage overload in "Avoiding and Managing Overload" in Oracle Fusion Middleware Configuring Server Environments for Oracle WebLogic Server at:

  http://download.oracle.com/docs/cd/E15523_01/web.1111/e13701/overload.htm

  For a description of how to replicate domain configuration files for managed server independence in, see "Replicate domain config files for Managed Server independence" in *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* at:

  http://download.oracle.com/docs/cd/E15523_01/apirefs.1111/e13952/taskhelp/domainconfig/ReplicateDomainConfigFilesForManagedServerIndependence.html

  For a description of server migration see "High Availability for WebLogic Server" in *Oracle Fusion Middleware High Availability Guide* at:
  http://download.oracle.com/docs/cd/E15523_01/core.1111/e10106/toc.htm

- **Enable Services Gatekeeper reliability and recovery features.**

  See "Redundancy, Load Balancing, and High Availability" and "Geographic Redundancy" in *Oracle Communications Services Gatekeeper Concepts Guide*.

- **Back up Oracle Fusion Middleware WebLogic Server domain configuration.**

  See:

  - Enabling Automatic Configuration Backups
  - Storing the Domain Configuration Offline
  - Backing Up Domain Security Data
  - Backing Up Additional Configuration Files

- **Back up the Oracle Middleware Fusion database configuration.**

  For Oracle Fusion Middleware 11g, see "Backing Up Your Environment" in *Oracle Fusion Middleware Administrator's Guide 11g* at:

  http://download.oracle.com/docs/cd/E15523_01/core.1111/e10105/br_bkp.htm#ASADM376

  and"Recovering Your Environment" in *Oracle Fusion Middleware Administrator's Guide 11* at:

  http://download.oracle.com/docs/cd/E15523_01/core.1111/e10105/br_rec.htm#BCGCBGDJ

For Oracle Fusion Middleware 10g, see the Oracle WebLogic Server 10g documentation at:

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/sitemap.html

2

Backing Up the Domain Configuration

This chapter provides information on and explains procedures for backing up the primary configuration artifacts of a Oracle Communications Services Gatekeeper domain.

Overview of Domain Configuration Backup

Recovery from the failure of a server instance requires access to the domain's configuration and security data. Services Gatekeeper can be configured to perform certain domain backups automatically. The administrator must also perform a manual backup of the domain configuration artifacts and store those backups outside of the actual domain directory.

By default, the Administration Server stores a domain's primary configuration data in a file called *Domain_Home***/config/config.xml**, where *Domain_Home* is the root directory of the domain. The primary configuration file may reference additional configuration files for specific Oracle Fusion Middleware WebLogic Server services, such as JDBC and JMS. The configuration for specific services is stored in additional XML files in subdirectories of the *Domain_Home***/config** directory, such as *Domain_Home***/config/jms** and *Domain_Home***/config/jdbc**.

The Administration Server can automatically archive multiple versions of the domain configuration (the entire *Domain_Home***/config** directory). The configuration archives can be used for system restoration in cases where accidental configuration changes need to be reversed. For example, if an administrator accidentally removes a configured resource, the prior configuration can be restored by using the last automated backup.

The Administration Server stores a finite number of automated backups locally in *Domain_Home***/config**. For this reason, automated domain backups are limited in their ability to guard against data corruption, such as a failed hard disk. Automated backups also do not preserve certain configuration data that is required for full domain restoration, such as LDAP repository data and server start-up scripts. Oracle recommends that you also maintain multiple backup copies of the configuration and security offline, in a source control system, as described in "Backing Up Domain Security Data".

Enabling Automatic Configuration Backups

Follow these steps to enable automatic domain configuration backups on the Administration Server for your domain:

1. Access the Administration Console for your domain.

2. In the left pane of the Administration Console, select the name of the domain.
3. In the right pane, click the **Configuration** tab and then the **General** tab.
4. In the **Advanced Options** bar, click **Show**.
5. In the **Archive Configuration Count** box, enter the maximum number of configuration file revisions to save.
6. Click **Apply**.

When you enable configuration archiving, the Administration Server automatically creates a configuration JAR file archive each time the Administrator uses the **Activate Changes** button in the Administration Console to change the active configuration. The JAR file contains a complete copy of the previous configuration (the complete contents of the *Domain_Home*/**config** directory). JAR file archive files are stored in the *Domain_Home*/**configArchive** directory. The files use the naming convention **config-***number*.**jar**, where *number* is the sequential number of the archive.

When you save a change to a domain's configuration, the Administration Server saves the previous configuration in *Domain_Home*/**configArchive/config.xml#***n*. Each time the Administration Server saves a file in the **configArchive** directory, it increments the value of the #*n* suffix, up to a configurable number of copies - 5 by default. Thereafter, each time you change the domain configuration:

- The archived files are rotated so that the newest file has a suffix with the highest number.
- The previous archived files are renamed with a lower number.
- The oldest file is deleted.

Keep in mind that configuration archives are stored locally within the domain directory, and they may be overwritten according to the maximum number of revisions you selected. For these reasons, you must also create your own off-line archives of the domain configuration, as described in "Storing the Domain Configuration Offline".

Storing the Domain Configuration Offline

Although automatic backups protect against accidental configuration changes, they do not protect against data loss caused by a failure of the hard disk that stores the domain configuration or against accidental deletion of the domain directory. To protect against these failures, also store a complete copy of the domain configuration offline.

Oracle recommends storing a copy of the domain configuration at regular intervals. For example, back up a new revision of the configuration when:

- You first deploy the production system.
- You add or remove deployed applications.
- The configuration is tuned for performance.
- Any other permanent change is made.

The domain configuration backup should contain the complete contents of the *Domain_Home*/**config** directory. For example:

```
cd Domain_Home/user_projects/domains/mydomain
tar cvf domain-backup-06-17-2007.jar config
```

Store the new archive in a source control system, preserving earlier versions should you need to restore the domain configuration to an earlier point in time.

Backing Up Domain Security Data

The Oracle Fusion Middleware security service stores its configuration data **config.xml** file and also in an LDAP repository and other files. As with the *Domain_Home*/**config** directory, a copy of the LDAP repository and security files should be stored offline each time you make a change to the security configuration.

Backing Up the Oracle Fusion Middleware LDAP Repository

The default Authentication, Authorization, Role Mapper, and Credential Mapper providers that are installed with Services Gatekeeper store their data in an LDAP server. Each Services Gatekeeper server instance contains an embedded LDAP server. The Administration Server contains the master LDAP server, which is replicated on all Managed Servers. If any of your security realms use these installed providers, you should maintain an up-to-date backup of the following directory tree:

Domain_Home/**servers**/*adminServer*/**data/ldap**

where *Domain_Home* is the domain's root directory and *adminServer* is the directory in which the Administration Server stores runtime and security data.

Each Services Gatekeeper server has an LDAP directory, but you only need to back up the LDAP data on the Administration Server. The master LDAP server replicates the LDAP data from each Managed Server when updates to security data are made. Oracle Fusion Middleware security providers cannot modify security data while the domain's Administration Server is unavailable. The LDAP repositories on Managed Servers are replicas and cannot be modified.

The **ldap/ldapfiles** subdirectory contains the data files for the LDAP server. The files in this directory contain user, group, group membership, policies, and role information. Other subdirectories under the **ldap** directory contain LDAP server message logs and data about replicated LDAP servers.

Do not update the configuration of a security provider while a backup of LDAP data is in progress. If a change is made - for instance, if an administrator adds a user - while you are backing up the **ldap** directory tree, the backups in the **ldapfiles** subdirectory could become inconsistent. If this does occur, consistent but potentially out-of-date LDAP backups are available.

Once a day, a server suspends write operations and creates its own backup of the LDAP data. It archives this backup in a ZIP file below the **ldap/backup** directory and then resumes write operations. This backup is guaranteed to be consistent, but it might not contain the latest security data.

For information about configuring the LDAP backup, see "Configure backups for embedded LDAP servers" in *Oracle Fusion Middleware Oracle WebLogic Server Administration Console Online Help* at:

http://download.oracle.com/docs/cd/E15523_01/apirefs.1111/e13952/taskhelp/security/ConfigureBackupsForEmbeddedLDAPServers.html

Backing Up SerializedSystemIni.dat and Security Certificates

All servers create a file named **SerializedSystemIni.dat** and place it in the *Domain_Home*/**security** directory. This file contains encrypted security data that must be present to boot the server. You must back up this file.

If you configured a server to use SSL, also back up the security certificates and keys. The location of these files is user-configurable.

Backing Up Additional Configuration Files

Certain additional files maintained at the operating system level can be helpful when recovering from a system failure. Consider backing up the following information as necessary for your system:

- Load Balancer configuration scripts. For example, any automated scripts used to configure load balancer pools and virtual IP addresses for the engine tier cluster, as well as NAT configuration settings.
- NTP client configuration scripts used to synchronize the system clocks of engine and data tier servers.
- Host configuration files for each Services Gatekeeper machine: host names, virtual and real IP addresses for multihomed machines, IP routing table information.
- Managed Server start scripts. In a Services Gatekeeper deployment, the start scripts used to boot Access and Network tier servers are generally customized to include configuration information such as JVM Garbage Collection parameters and other tuning parameters.

As with offline backups of the domain configuration, Oracle recommends storing multiple copies of the above files in a source control repository.

3

Restoring Failed Server Instances

This chapter provides information on and procedures for restoring and moving failed servers in a Oracle Communications Services Gatekeeper domain.

Restarting a Failed Administration Server

When you restart a failed Administration Server, no special steps are required. Start the Administration Server as you normally would.

If the Administration Server shuts down while Managed Servers continue to run, you do not need to restart the Managed Servers that are already running in order to recover management of the domain. The procedure for recovering management of an active domain depends upon whether you can restart the Administration Server on the same machine it was running on when the domain was started.

Restarting an Administration Server on the Same Machine

If you restart the Services Gatekeeper Administration Server while Managed Servers continue to run, by default the Administration Server can discover the presence of the running Managed Servers.

When starting the server, make sure that the startup command or startup script does not include the `-Dweblogic.management.discover=false` option, which prevents an Administration Server from discovering its running Managed Servers.

The root directory for the domain contains a file, **running-managed-servers.xml**, which contains a list of the Managed Servers in the domain and describes whether they are running. When the Administration Server restarts, it checks this file to determine which Managed Servers were under its control before it stopped running.

When a Managed Server is gracefully or forcefully shut down, its status in **running-managed-servers.xml** is updated to NOT-RUNNING. When an Administration Server restarts, it does not try to discover Managed Servers with the "not-running" status. A Managed Server that stops running because of a system crash, or that was stopped by killing the JVM or the command prompt (shell) in which it was running still has the status RUNNING in **running-managed-servers.xml**. The Administration Server attempts to discover non-running servers and throws an exception when it determines that the Managed Server is no longer running.

Restarting the Administration Server does not cause Managed Servers to update the configuration of static attributes. Static attributes are those that a server refers to only during its startup process. Servers instances must be restarted to take account of changes to static configuration attributes. Discovery of the Managed Servers enables the Administration Server only to monitor the Managed Servers or make runtime

changes in dynamic attributes, which are those that can be configured while a server is running.

Restarting an Administration Server on Another Machine

If a machine crash prevents restarting the Administration Server on the same machine, you can recover management of the running Managed Servers as follows:

1. Install the Services Gatekeeper software on the new administration machine, if this has not already been done.
2. Make the application files available to the new Administration Server by copying them from backups or by using a shared disk. Application files should be available in the same relative location on the new file system as on the file system of the original Administration Server.
3. Make configuration and security data available to the new administration machine by copying them from backups or by using a shared disk. For more information, refer to "Storing the Domain Configuration Offline".
4. Restart the Administration Server on the new machine.

   Make sure that the startup command or startup script does not include `-Dweblogic.management.discover=false`, which disables an Administration Server from discovering its running Managed Servers.

When the Administration Server starts, it communicates with the Managed Servers and informs them that the Administration Server is now running on a different IP address.

Restarting Failed Access and Network Tier Servers

If the machine on which the failed Managed Server runs can contact the Administration Server for the domain, restart the Managed Server manually or automatically using Node Manager. Note that you must configure Node Manager and the Managed Server to support automated restarts, as described in "Using Node Manager" in *Oracle Fusion Middleware Node Manager Administrator's Guide for Oracle WebLogic Server* at:

`http://download.oracle.com/docs/cd/E15523_01/web.1111/e13740/starting_nodemgr.htm`

If the Managed Server cannot connect to the Administration Server during startup, it can retrieve its configuration by reading locally-cached configuration data. A Managed Server that starts in this way is running in Managed Server Independence (MSI) mode. For a description of MSI mode, and the files that a Managed Server must access to start up in MSI mode, see "Understanding Managed Server Independence Mode" in *Oracle Fusion Middleware Managing Server Startup and Shutdown for Oracle WebLogic Server* in:

`http://download.oracle.com/docs/cd/E15523_01/web.1111/e13708/failures.htm#START185`.

To start up a Managed Server in MSI mode:

1. Ensure that the following files are available in the Managed Server's root directory:
   - **msi-config.xml**.
   - **SerializedSystemIni.dat**
   - **boot.properties**

If the files are not in the Managed Server's root directory, do one of the following:

a. Copy the **config.xml** and **SerializedSystemIni.dat** file from the Administration Server's root directory (or from a backup) to the Managed Server's root directory.

b. Rename the configuration file **msi-config.xml**. When you start the server, it will use the copied configuration files.

or

- Use the `-Dweblogic.RootDirectory=path` startup option to specify a root directory that already contains the**config.xml** and **SerializedSystemIni.dat** files.

2. Start the Managed Server at the command line or using a script.

   The Managed Server will run in MSI mode until it is contacted by its Administration Server. For information about restarting the Administration Server in this scenario, see "Restarting a Failed Administration Server".

Moving an Access or Network Tier Server to a Different Machine

Sometimes it is necessary to restart an Access tier or Network tier server instance on a different machine. This situation might occur if a server machine's motherboard fails or if you upgrade to newer server hardware. When restarting a server on a new machine, maintain the same IP address and network configuration (DNS name, port numbers, and so forth) as the previous machine, if possible. If the network configuration remains unchanged, the server can accept the existing domain configuration and you can restart it using the techniques described in "Restarting Failed Access and Network Tier Servers".

If the network configuration is changed on the newer machine, you must update the domain network configuration to match the server machine. Follow these steps before booting either an Access tier or Network tier server:

1. Access the Administration Console for the domain.
2. Click the **Lock & Edit** button to start a configuration session.
3. Click the **Environment** tab and then the **Servers** tab in the left pane.
4. Select the name of the server to update from the list of servers in the right pane.
5. Click the **Configuration** tab and then the **General** tab. Modify the listen address and port settings to match the new server hardware.
6. Click the **Protocols** tab and then the **Channels** tab. Modify any configured network channels to match the network settings of the new server hardware.
7. Click **Activate Changes** to apply your configuration changes.
8. Start the Managed Server on the new server hardware, using the instructions in "Restarting Failed Access and Network Tier Servers".

In addition to the preceding steps, Network tier servers require that you update the routing configuration for backwards compatible communication service plug-ins. This is required because the routing configuration uses Network tier servers' IP addresses in the plug-in ID. Remove any old routes that involve the affected Network tier server, and create new routes based on the new server machine's network configuration. For more information, see "Managing and Configuring the Plug-in Manager" in Oracle Communications Services Gatekeeper *System Administrator's Guide*, another document in this set.

A

Oracle Communications Services Gatekeeper Tables

This appendix lists all the tables that are created on first start-up of the Oracle Communications Services Gatekeeper database (except deployment-specific tables), and backward-compatible tables.

As an optimization, it is possible to remove tables if your communication services do not require them. Because non-existent tables do not require backing up, this makes your implementation more efficient.

Standard Service Gatekeeper 5.1 Tables

WLS_ACTIVE

BUDGET_CONFIG_TABLE

BUDGET_SERVICE_STATE_TABLE

BULK_MMS_CHUNK_LIST

BULK_MMS_CHUNK_SUB_LIST

BULK_MMS_ORDER_LIST

BULK_PUSH_CHUNK_LIST

BULK_PUSH_ORDER_LIST

BULK_PUSH_CHUNK_SUB_LIST

BULK_SMS_CHUNK_LIST

BULK_SMS_CHUNK_SUB_LIST

BULK_SMS_ORDER_LIST

CC_INTERCEPTOR_DATA

GLOBAL_BUDGET_CONFIG_TABLE

GLOBAL_WLNG_SLAS

LEGACY_SMPP_CONNECTION_STORE

LEGACY_SMPP_NOTIF_STORE

LEGACY_SMPP_SESSION_STORE

MPCC_CALL_LEG_SESSION

MPCC_CALL_SESSION

NATIVE_SMPP_SESSION_STORE

PL_AC_SIP_STATUS

PL_CD_SIP_ADDR_COR

PL_CD_SIP_COR_SUB

PL_CN_PX30_OSA_ASSOCIATOR

PL_CN_PX30_OSA_INFO

PL_CN_SIP_ADDR_COR

PL_CN_SIP_COR_SUB

PL_LEGACY_MM7_NOTIF

PL_LEGACY_MMS_MT

PL_MMS_MO_CONTENT_MMS

PL_MMS_MO_MMS

PL_MMS_MT_DR_MMS

PL_MMS_OFFLINE_NOTIF

PL_MMS_ONLINE_NOTIF

PL_LEGACY_MMS_STATUS

PL_LEGACY_MMS_VASP_ID

PL_LEGACY_MMS_VAS_ID

PL_LEGACY_SMPP_BIND_STORE

PL_MPCC_MEDIA_NOTIF

PL_SMS_ONLINE_NOTIF

PL_SMS_SMPP_MO_SMS

PL_PAYMENT_RESERVATION_DATA

PL_PUSH_PAP_NOTIFICATION_INFO

PL_PX30_AC_UI_CALL_INFO

PL_PX30_UI_CALL_LEG_INFO

PL_SMS_BINARY_NOTIF

PL_SMS_MO_SMS

PL_SMS_OFFLINE_NOTIF

PL_SMS_SMPP_MT_SMS

PL_TL_MLP_TRIGGER_INFO

PL_TPC_INAP

PL_TS_MAP_NETWRK

PL_TS_MAP_NETWRK_ROUTE

PL_TS_MAP_NOTIF

PL_TS_MAP_TRIGGERS

PRES_SIP_NOT

PRES_SIP_SUB

PRES_SIP_URI_MAP

PRM_USERS_BC

SHORTCODE_MAPING_STORE

SLEE_ALARM

SLEE_CHARGING

SLEE_INSTANCE_IDS

SLEE_LICENSE_TPS_LOG

SLEE_PL_MGR_PLUGIN

SLEE_SNMP_CONFIG

SLEE_SNMP_TRAP_RECEIVERS

SLEE_STATISTICS_DATA

SLEE_SUPPORTED_STATISTICS

SMPP_SERVICE_APP_INFO

SLEE_DB_LOCKS

SLEE_LICENSE_TPS_CHECK_STATE

SLEE_STATISTICS_CONFIG

SMPP_SERVICE_MO_CON

TPC_CALL_PARTICIPANTS_INFO

TPC_SIP_CALLSESSION_INFO

WLNG_ACCOUNT_GROUPS

WLNG_APP_ACCOUNTS

WLNG_APP_INSTANCES

WLNG_APP_SESSIONS

WLNG_BLOB_CONFIGURATION

WLNG_CONFIGURATION

WLNG_HTTPPROXY

WLNG_MGMT_USERGROUPS

WLNG_MGMT_USERS

WLNG_PRM_SESSIONS

WLNG_SLA_CUSTOM_XSD

WLNG_SLAS

WLNG_SP_ACCOUNTS

WLNG_SUBSCR_CONTRACTS

Services Gatekeeper Backwards Compatible Tables

If you are using backwards compatible listeners (CORBA-based) for alarms, EDRs, or CDRs, there are additional tables in the database. These tables are not included by default in the out-of-the-box version of Services Gatekeeper.

slee_alarm_config

slee_alarm_params

slee_alarm_severity_mapping

slee_charging_config

slee_charging_listeners

slee_edr_filter_properties

slee_edr_filters

slee_edr_listener_filters

slee_edr_listeners