Oracle® Communications Services Gatekeeper

Multi-tier Installation Guide

Release 6.0

E50756-03

November 2015

ORACLE®

Oracle Communications Services Gatekeeper Multi-tier Installation Guide, Release 6.0

E50756-03

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents ix

1 Services Gatekeeper Installation Overview

Overview of Installed Components 1-1
Overview of the Services Gatekeeper Installation Procedure 1-1
Services Gatekeeper Installation Options 1-2
Ensuring a Successful Services Gatekeeper Installation 1-3
Placeholders Used in this Guide 1-3

2 Planning Your Services Gatekeeper Installation

About Services Gatekeeper Software Components 2-1
Understanding Services Gatekeeper Domains 2-2
Overview of Deployment Types 2-3
About Tiered Deployments 2-4
Physical Architecture 2-5
Runtime Aspects 2-6
Scalability 2-7
Security 2-7
High Availability 2-8
About Non-tiered Deployments 2-8
Using Non-tiered Deployments in Production Environments 2-8
Using Non-tiered Deployments in Test and Development Environments 2-9
About Geographically Redundant Deployments 2-10
About Domain Configuration Templates for Deployment Types 2-11
System Deployment Planning 2-13
About Setting Up Services Gatekeeper Reporting Support 2-13
About Deploying Partner Relationship Management Modules 2-14
About Integrating Services Gatekeeper with Service Controller 2-15
About Enterprise Manager Compatibility 2-15
About XML Applications 2-16
About Deployment Administration 2-17
Disk Storage Planning 2-18

Latency and Bandwidth Requirements 2-18
Latency Requirements 2-18
Bandwidth Requirements 2-18
Database Planning 2-18

3 Services Gatekeeper System Requirements

Software Requirements 3-1
Supported Databases 3-1
Supported Virtualization Software 3-2
Supported Protocols 3-2
About Critical Patch Updates 3-2
Hardware Requirements 3-3
Information Requirements 3-3

4 Installing the Database

Database Installation Overview 4-1
Installing Oracle RAC or Oracle Single Instance Database Software 4-1
About Using Oracle RAC with WebLogic Server 4-1
Installing the Database Software 4-1
Setting Up a Services Gatekeeper User for the Oracle Database 4-2
Installing Oracle Database Express Edition 4-2
Installing the Oracle XE Software 4-2
Configuring Oracle XE for Services Gatekeeper 4-3
Installing MySQL Database 4-3
Installing the MySQL Database Software 4-4
Configuring MySQL on Linux 4-4
Configuring MySQL on Windows 4-5
Creating the Database and a Database User 4-5
Installing MySQL Cluster CGE 4-6
Installing the MySQL Cluster CGE Software 4-6
Configuring the Management Server Node 4-6
Starting the MySQL Cluster Processes 4-7

5 Installing Services Gatekeeper

About Installing Services Gatekeeper 5-1
Installation Prerequisites 5-1
Installing the JDK 5-1
Setting the Java Path 5-1
Creating an Installation Log 5-2
Installing Services Gatekeeper in GUI Mode 5-2
Installing Services Gatekeeper in Silent Mode 5-4
About the Response File 5-4
Returning Exit Codes to the Console 5-5
Running the Installer in Silent Mode 5-6
Where to Go from Here 5-6

6 Services Gatekeeper Post-Installation Tasks

Overview of Services Gatekeeper Post-Installation Tasks 6-1
Setting the WebLogic Server Home Path 6-1
Configuring Your Services Gatekeeper Domain 6-1
Post-Installation Tasks for Services Gatekeeper 6-2
Creating JMS Servers for Additional Network Tier Servers 6-2
(Optional) Adding a Custom Password Validator 6-3
(Optional) Adding Java Cryptography Extensions 6-4
Post-Installation Tasks for Reports 6-4
Configuring the Reports Data Source 6-4
Configure EDRs 6-5
Deploying the Reports EAR File 6-6
Connecting Services Gatekeeper to the Reports Data Source 6-7
Verifying the Services Gatekeeper Installation 6-7
Where to Go from Here 6-8

7 Configuring the Services Gatekeeper Domain

About Configuring Service Gatekeeper Domains 7-1
About the Domain Configuration Tools 7-1
Information Requirements 7-2
Supporting Dual-Stack IPv4/IPv6 Traffic 7-2
Configuring the Domain Using the Configuration Wizard in GUI Mode 7-2
Mapping Host Names to IPv6 Addresses 7-2
Starting the Configuration Wizard in GUI Mode 7-3
Configuring the Domain in GUI Mode 7-3
Configuration Type Screen 7-4
Templates Screen 7-4
Administrator Account Screen 7-4
Domain Mode and JDK Screen 7-5
JDBC Data Sources Screen 7-5
JDBC Data Sources Test Screen 7-6
Advanced Configuration Screen 7-6
Configuration Summary Screen 7-7
Configuration Progress Screen 7-7
Configuration Success Screen 7-7
Configuring the Domain Using the Configuration Wizard in Console Mode 7-7
Starting the Configuration Wizard in Console Mode 7-7
Configuring the Domain in Console Mode 7-8
Configuring the Domain Using a WebLogic Scripting Tool Script 7-8
Setting Up Your Environment 7-8
Choosing the WLST Domain Setup Script 7-9
Configuring the WLST Script 7-9
Configuring Multicluster Settings 7-9
Adding Machines and Servers to a Multicluster Configuration 7-11
Preventing Communication Services from Being Deployed 7-13
Running the WLST Domain Setup Script 7-13

Where to Go From Here 7-13

8 Installing Services Gatekeeper Reports

Overview of Installing Services Gatekeeper Reports 8-1
Reports System Requirements 8-1
Installation Prerequisites 8-1
Installing Oracle Business Intelligence 8-2
Configuring Oracle Business Intelligence 8-2
Setting Configuration Permissions 8-2
Creating the Reports Repository Database and User 8-2
Configuring the Services Gatekeeper RPD File 8-3
Gathering Required Oracle Business Intelligence System Information 8-3
Installing Services Gatekeeper Reports 8-3
Enabling Oracle Business Intelligence Write-Back and Iframe Support 8-6
Configure OBIEE Caching For Improved Performance 8-7
Where to Go from Here 8-7

9 Installing the Platform Test Environment

Overview of Installing PTE 9-1
Installing the PTE in GUI Mode 9-1
Installing the PTE in Silent Mode 9-2
Where to Go from Here 9-3

10 Installing the Application Test Environment

Overview of Installing Services Gatekeeper Application Test Environment 10-1
ATE System Requirements 10-1
Setting Your Environment Variables for ATE 10-1
Installing the ATE in GUI Mode 10-2
Installing the ATE in Silent Mode 10-3
Where to Go from Here 10-4

11 Upgrading Services Gatekeeper

About Upgrading Services Gatekeeper 11-1
Upgrade Restrictions 11-2
Placeholders Used in This Chapter 11-2
Upgrading Servers 11-2
Deploying New Services Gatekeeper Applications 11-8
Cleaning Up Files After Upgrading 11-10
Upgrading Services Gatekeeper Reports 11-11
Upgrade Troubleshooting 11-12
A Network Tier Server Cannot Rejoin Its Coherence Cluster 11-12
A Network Tier Server Cannot Rejoin Its Services Gatekeeper Cluster 11-13
Administration Console Pages are Not Displayed Properly 11-13

12 Patch Management of Services Gatekeeper Systems

About Services Gatekeeper Patch Releases 12-1
Types of Patch Releases 12-1
About Patch Sets 12-1
About Debug Patches 12-1
About Temporary Fixes 12-2
Finding Your Current Patch Level 12-2
About Patch Content 12-2
About Patch Management In Clustered Environments 12-2
About OPatch 12-3
Requirements for OPatch 12-3
Managing a Patch Release Installation Process 12-3
Preparing to Install the Patch 12-3
Verifying the Oracle Universal Installer Inventory 12-3
Creating a Backup of Your Current Services Gatekeeper Installation 12-4
Checking Your Environment Variables 12-4
Creating a Location for the Patch 12-4
Stopping All WebLogic Servers 12-4
Installing the Patch 12-4
Completing Patch Installation 12-5
Troubleshooting 12-5
Uninstalling the Patch 12-6
OPatch Utility Reference 12-6
Dealing with Conflicts When You Run the Apply Command 12-7

13 Uninstalling Services Gatekeeper

Uninstalling Services Gatekeeper Components in GUI Mode 13-1
Uninstalling Services Gatekeeper Components in Silent Mode 13-2

14 Next Steps

Configuring Services Gatekeeper 14-1

Preface

This book explains how to install Oracle Communications Services Gatekeeper. It includes instructions for WebLogic Server domain configuration and post-installation tasks.

Audience

The person installing the software should be familiar with the following topics:

- Operating system commands
- Database configuration
- WebLogic Server

Before reading this guide, you should have a familiarity with Services Gatekeeper. See *Services Gatekeeper Concepts*.

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 Concepts*
- *Oracle Communications Services Gatekeeper Licensing Guide*
- *Oracle Communications Services Gatekeeper Security Guide*
- *Oracle Communications Services Gatekeeper System Administrator's Guide*

For related information about Oracle WebLogic Server 11*g* or 12*c*, see the following documents:

- *Oracle Fusion Middleware Introduction to Oracle WebLogic Server*

- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*
- *Oracle Fusion Middleware Managing Server Startup and Shutdown for Oracle WebLogic Server*
- *Oracle Fusion Middleware Using Clusters for Oracle WebLogic Server*
- *Oracle Fusion Middleware Securing Oracle WebLogic Server*

The Oracle WebLogic Server 11*g* and 12*c* documentation are available on the Oracle WebLogic Server Product Documentation page of the Oracle Technology Network website:

http://www.oracle.com/technetwork/middleware/weblogic/documentation/index.html

1

Services Gatekeeper Installation Overview

This chapter describes the general process of installing and configuring Oracle Communications Services Gatekeeper.

To learn more about installing WebLogic Server products in general, and about the installer program in particular in regard to WebLogic Server, see *Installing and Configuring Oracle WebLogic Server and Coherence Software* at the Oracle Fusion Middleware Documentation website.

Overview of Installed Components

During the installation process, you install and configure the following components:

- Your database
- The Services Gatekeeper software, which includes:
  - Container services and communication services applications
  - Portal Server
  - Platform Development Studio (PDS)
  - WebLogic Server, which is the platform container
- (Optional) Services Gatekeeper Application Test Environment (ATE)
- (Optional) Services Gatekeeper Platform Test Environment (PTE)
- (Optional) Services Gatekeeper Reports

Overview of the Services Gatekeeper Installation Procedure

The installation procedure follows these steps:

1. Plan your installation. When planning your installation, do the following:
   - Determine the scale of your implementation, for example, a small development system, or a large production system.
   - Determine how many physical machines you need, and which software components to install on each machine.
   - Plan the system topology, for example, how the system components connect to each other over the network.
2. Review system requirements. System requirements include:
   - Hardware requirements, such as processor and disk space.

- System software requirements, such as operating system (OS) versions and OS patch requirements.
- Information requirements, such as IP addresses and host names.

3. Perform pre-installation tasks such as installing the database and the JDK.
4. Install Services Gatekeeper.

   When you install Services Gatekeeper, WebLogic Server is also installed.
5. Perform post-installation tasks:
   - Configure your domains.
   - Install optional Services Gatekeeper components, such as Reports, Application Test Environment, and Platform Test Environment.
   - Perform additional configuration tasks.
6. Verify the installation.
7. If you are upgrading from a previous version of Services Gatekeeper, perform the upgrade tasks. See "Upgrading Services Gatekeeper" for more information.

After Services Gatekeeper is installed, perform some system administration tasks such as the following tasks, among others:

- Configure system security, including user names and passwords.
- Configure container services and communication services.
- Set up service provider and application accounts and service level agreements (SLAs).

Services Gatekeeper Installation Options

When installing Services Gatekeeper, you can use the following types of installation:

- Single-tier installation

  The single-tier (default) installation installs a preconfigured Services Gatekeeper implementation that includes everything you must run a test system, or a small to medium size production environment on a single system. This is the fastest installation option and also appropriate for test and evaluation systems. It includes a Services Gatekeeper Administration Server, managed server (with integrated network and access tiers), and a Java DB database.

  The single-tier installation supports GUI mode only.
- Multi-tier installation

  A multi-tier installation is appropriate for deployments where the Access Tier and Network Tier servers are in separate clusters. There are two installer modes for multi-tier installations:

  – GUI mode: An interactive mode that uses a graphical user interface

  – Silent mode: A non-interactive mode that uses a script and an XML input file

    Silent mode is a way of setting installation options once and then using those settings to duplicate the installation on many systems. The installation program reads your settings from a file that you create prior to beginning the installation. The installation program does not display any options during the installation process. Silent-mode installation works on Windows, Linux, and Solaris systems.

Ensuring a Successful Services Gatekeeper Installation

The Services Gatekeeper installation should be performed only by qualified personnel. You must be familiar with Oracle WebLogic Server and the supported operating systems. You should be experienced with installing Java-related packages. Oracle recommends that the Oracle database installation and configuration be performed by an experienced database administrator.

Follow these guidelines:

- As you install each component (for example, the Oracle database), verify that the component installed successfully before continuing the installation process.
- Pay close attention to the system requirements. Before you begin installing the software, make sure your system has the required base software. In addition, make sure that you know all of the required configuration values, such as host names and port numbers.
- As you create new configuration values, write them down. In some cases, you might need to re-enter configuration values later in the procedure.

Placeholders Used in this Guide

Table 1–1 shows the placeholders used in this guide:

Table 1–1 Placeholders Used Throughout Documentation

Placeholder	Description
Middleware_home	The directory that serves as the repository for common files that are used by Oracle Communications products installed on the same system, such as Services Gatekeeper and WebLogic Server. The files in the *Middleware_home* directory are essential to ensuring that software operates correctly on your system. They: ■ Facilitate checking of cross-product dependencies during installation ■ Facilitate Service Pack installation
Services_Gatekeeper_home	The directory in which the Services Gatekeeper software is installed. By default, this is a subdirectory of *Middleware_home*; for example, *Middleware_home***/ocsg**.
domain_home	The directory in which the Services Gatekeeper domain resides, located in *Middleware_home***/user_projects/domains**.
installer_file	The product installation file that you download and run to install the software.

2

Planning Your Services Gatekeeper Installation

This chapter provides information about planning your Oracle Communications Services Gatekeeper installation.

About Services Gatekeeper Software Components

Services Gatekeeper is built on top of Oracle WebLogic Server and can use all WebLogic Server components. It also embeds Oracle Communications Converged Application Server for connectivity to SIP networks and access to network nodes using the Diameter protocol.

Services Gatekeeper provides communication services that telecom operator in-house applications and third-party applications use to access assets in the telecom network. For a list of the supported communication services, see *Services Gatekeeper Communication Service Reference Guide*. In addition, Services Gatekeeper provides extension points and tooling that you can use to create new communication services.

Each communication service has two components:

- A service facade that exposes interfaces to be used by applications.
- A service enabler that consists of a network protocol plug-ins. The plug-ins can be instantiated. Each instance connects to a node in the telecom network using a specific protocol. These instances interact with container services as necessary.

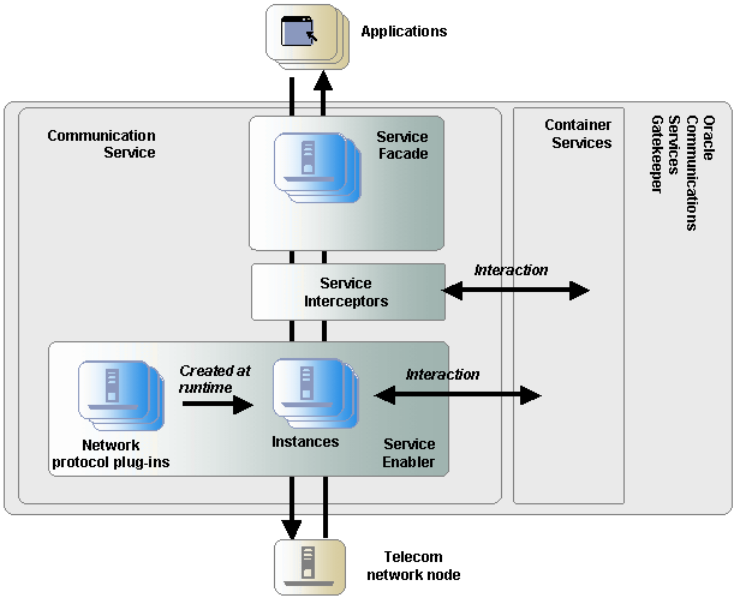
The communication services use container services, which are provided with the installation. Container services include Alarm, Event Data Record (EDR), Call Details Record (CDR), Policy Enforcement, Service Level Agreement (SLA) enforcement, Account, Event channel, and Trace services.

Requests between the network and applications can be intercepted by using service interceptors, which may allow, deny, or manipulate the request as necessary. When called upon to act on a request, service interceptors interact with container services as necessary to determine how to handle the request.

Service facades, service enablers, and service interceptors are deployable units in Services Gatekeeper.

Figure 2–1 illustrates how the Services Gatekeeper service components mediate the flow of requests between applications and the telecom network node.

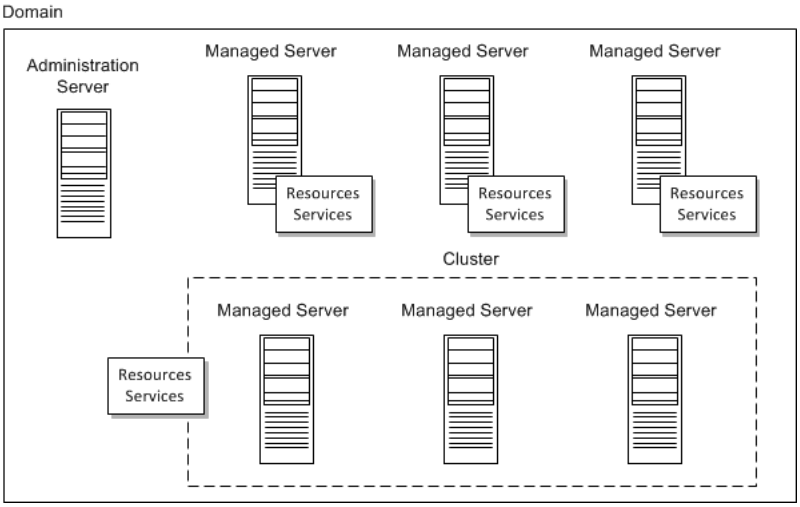
Figure 2–1 Services Gatekeeper Components



Understanding Services Gatekeeper Domains

A domain is the basic administrative unit in Oracle WebLogic Server. It consists of an Administration Server and, usually, one or more managed servers, which may be grouped into clusters, as illustrated in Figure 2–2.

Figure 2–2 WebLogic Domain



The Administration Server is used to manage the domain and provides access to the WebLogic Server administration tools.

A single WebLogic Server instance can function as both the Administration Server and a managed server, depending on the purpose of the installation. For example, developers creating communication service extensions using the Platform Development Studio might run both the Administration Server and managed servers on a single machine.

Managed servers are often grouped together into clusters that work together to provide scalability and high availability. Clusters improve performance and provide failover should a server instance become unavailable. The servers within a cluster can run on the same machine, or they can reside on different machines. To the client, a cluster appears as a single WebLogic Server instance.

Managed servers, or the clusters to which they are linked, host application components—in this case, the communication services—and resources, which are also deployed and managed as part of the domain.

Each server instance is also assigned to a machine that is a logical representation of actual hardware. The machine representation is used by the Administration Server to start and stop remote servers using the node manager. Multiple server instances can run in a single machine.

For more information about WebLogic Server domains, see "WebLogic Server Domains" in the WebLogic Server documentation.

Overview of Deployment Types

Services Gatekeeper supports the following types of deployments:

- Tiered deployments, which are suitable for large production environments
- Non-tiered deployments, which are suitable for test and development and small-scale production environments. There are two types of non-tiered deployments:
  - basic developer
  - basic high availability
- Geographically redundant deployments, which are suitable for large production environments in which provisioning and run-time processing data are replicated between sites

Table 2–1 provides a summary of the different deployment types.

Table 2–1 Summary of Deployments

Deployment Type	Provides	Characteristics
Tiered	Access and Network clusters	Targeted for medium and large deployments. Some high-availability aspects. High level of security. High level of scalability.

Table 2–1 (Cont.) Summary of Deployments

Deployment Type	Provides	Characteristics
Non-tiered	Basic developer configuration	Targeted to extension and integration developers. No high-availability or redundancy aspects.
Non-tiered	Basic high-availability	Targeted for smaller deployments, testing, and development. Introduces support for high availability or redundancy.
Geographic redundancy	Geographically separated sites with data synchronization	Each site has the characteristics of a tiered deployment. Adds geographic redundancy aspects that allow for disaster failover in the event of a site failure. Both sites are active; assumes site affinity from an application's point of view.

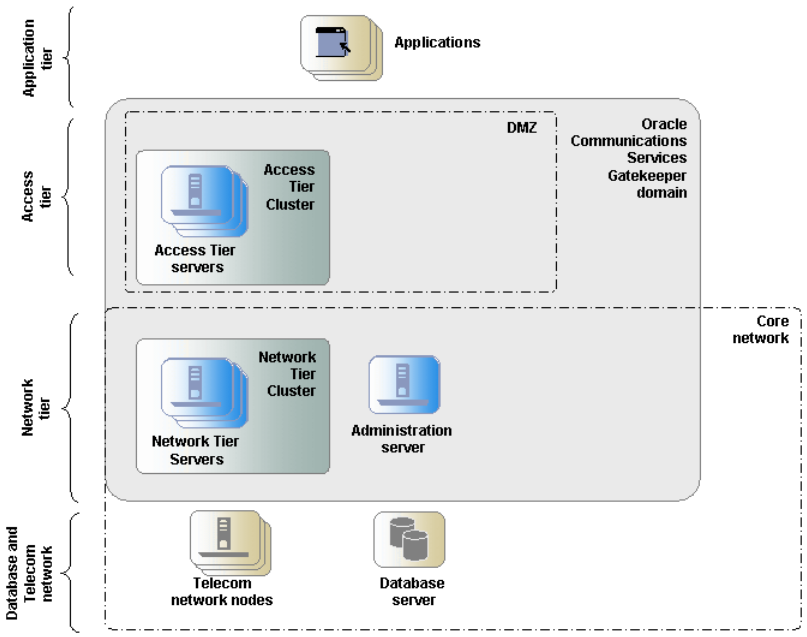
About Tiered Deployments

A Services Gatekeeper deployment is normally divided into three tiers: the Access Tier, the Network Tier, and the database tier.

As Figure 2–3 shows, in-house and third-party applications that use Services Gatekeeper interact only with the Access Tier. The Network Tier interacts with the telecommunications network, the Access Tier, and other nodes such as Operation Support Systems (OSS) or Business Support Systems (BSS).

Service facades are deployed in the Access Tier nodes. Service enablers and container services are deployed in the Network Tier nodes.

Figure 2–3 Example of a Tiered Deployment



The tiering physically separates the servers, which enables carrier-grade scaling, security, and high availability.

Services Gatekeeper uses storage services that rely on an underlying database. For security reasons and in order to scale the database tier independently, the database is normally running on separate, dedicated nodes.

Physical Architecture

Each deployment consists of a number of nodes to ensure high availability and to provide redundancy and load balancing. The nodes are separated into a tiered architecture.

Production deployments of Services Gatekeeper are normally tiered into an Access Tier, a Network Tier, and a database tier.

The Access Tier is responsible for:

- Security
- SSL (secure sockets layer) termination
- XML serialization
- Termination of more latent WAN connections with applications

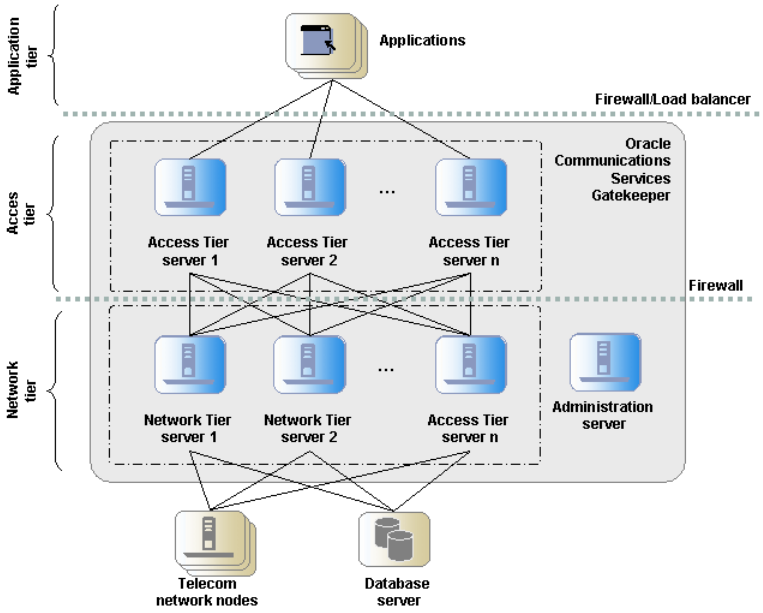
The Network Tier is responsible for:

- Network protocol translation
- Generation of EDRs (event data records), CDRs (charge data records), and alarms
- Inter-node communications and state management

The database tier is a relational database management system (RDBMS) used to store configuration and provisioning data, as well as data generated as a result of interaction with applications and network nodes. The RDBMS is abstracted by the Storage Service, a container service that provides the nodes with access to a shared cache. The Storage Service is deployed on nodes in the Network Tier.

Figure 2–4 shows an example of the tiered deployment of servers in a Services Gatekeeper installation. A firewall and a load balancer separates the application tier from the servers in the Access Tier. A second firewall regulates the traffic between the servers in the Access Tier and the servers at the Network Tier. All servers in the Network Tier are managed by the Services Gatekeeper Administration Server. The managed servers in the Network Tier can access the telecom network nodes and the database servers.

Figure 2–4 Servers in a Tiered Deployment



As seen in Figure 2–4, the tiers provide a separation at the network level, which allows for:

- Firewalls to be introduced between the tiers
- Different networks to be used for the different tiers

The servers are also physically separated within a tier.

Each tier consists of at least one cluster, with at least two server instances (nodes) per cluster, and all server instances run in active mode, independently of each other. The servers in all clusters are, in the context of Oracle WebLogic Server, managed servers. Together the clusters make up a single WebLogic Server administrative domain, controlled through an Administration Server.

Runtime Aspects

Nodes are grouped into one or more clusters in a deployment. With a few exceptions, all the same components are deployed on nodes within a cluster and these components are managed as one unit. There are a set of services where a component, a cluster singleton, is active only on one node within the cluster at any given point. In case of node failure, the singleton service is automatically migrated to another node in the cluster.

Configuration settings for a deployed module can be per node or shared among the components deployed in the a cluster.

The clusters are grouped into a domain, with an Administration Server that normally does not process any traffic. The traffic-processing nodes are called managed servers.

There is normally a one-to-one relationship between managed servers and a physical servers. In some cases, several managed servers can run on the same physical server. If the CPU is powerful and has a lot of memory, performance can benefit from using a smaller heap size for a set of managed servers on a single physical server, rather than

using one managed server per physical server. The disadvantage of this setup is mainly loss of redundancy and lower availability if a physical server fails.

Scalability

The Access Tier and the Network Tier scale independently of each other. New servers can be added at runtime, allowing you to scale the deployment horizontally.

The main responsibilities of the Access Tier are security, SSL termination, XML serialization and termination of WAN connections from applications. The main responsibilities of the Network Tier are to perform network protocol translation and protocol abstraction. This separation of responsibilities translates into two very different processing models.

Processing in the Access Tier is CPU-intensive, mainly concerned with XML to Java translations that have a short life span and generate numerous short-lived objects that trigger frequent garbage collection. The Access Tier does not maintain any state information. This behavior is consistent across communication services.

Processing in the Network Tier maintains state information and puts demands on data caching, inter-node communication, and processing logic.

The behavior of communication services varies with some of the services supporting relatively long-lived sessions. Call control sessions tend to have a significantly longer session lifetime than more data-centric sessions, such as messaging.

Some protocols, for example short message peer-to-peer protocol (SMPP), have more efficient data transfer sizes compared to XML-based protocols, for example multimedia messaging service interface (MM7). This translates into different processing needs.

Sizing and configuring individual servers in the Network Tier depend on which communication services are used in the deployment and the estimated utilization ratio between them. Both the physical characteristics of the servers (such as internal memory, network cards and CPU speeds) and settings for the Java Virtual Machine, (such as heap size and other parameters that affect garbage collection) can be optimized for the different use cases.

In summary, the processing models determine how you optimize the physical hardware, the Java Virtual Machine, and the operating system. Tiering allows you to tune individual nodes in each tier for the different processing requirements.

Security

Services Gatekeeper provides extensive support for authentication, authorization, and accounting. In addition, the separation of physical tiers allows for network-level security. This helps protect the network from attacks by fraudulent applications that use resources without paying for their usage and attacks designed to take resources out of service.

By using separate IP-network domains, one for the Access Tier and one for the Network Tier, you can apply different levels of network security. Applications are allowed to physically connect only to Access Tier servers, possibly fronted by a firewall, while the Network Tier servers only have access to the network domain where the telecommunication network nodes reside. In addition to this, the Access Tier servers are only allowed to connect to the Network Tier servers, possibly using a firewall between the tiers.

This topology puts the Access Tier servers in a demilitarized zone (DMZ) where out-of-network applications are only allowed access to the Access Tier servers. It also

puts the Network Tier servers in a more strictly controlled domain, where the network elements they connect to are well known and the access is controlled by firewalls.

High Availability

From a high-availability perspective, tiered deployments are better than non-tiered deployments. Processing in the Access Tier is stateless and is characterized by negligible latency while processing in the Network Tier is stateful, involves more processing logic, and higher latency.

In a tiered deployment, the Access Tier adds a high-level load balancing function that is aware of the health of each Network Tier server and quickly removes an out of service server from the list of servers to load balance among. This means that fewer requests are affected if a fault occurs.

The Access Tier guarantees that requests toward the Network Tier are properly load balanced and are not repeatedly sent to Network Tier servers that are out of service. Network tier servers asynchronously update the Access Tier servers when they are back in service.

If a request from an Access Tier server targets a Network Tier server that has failed, the Access Tier server sends the request to another Network Tier server. The Storage Service provides reliable cluster-wide access to all state information kept by the Network Tier. As a result, any Network Tier server can process requests coming from any Access Tier node or network node. If a node fails, cluster singleton services are automatically migrated from the failed node to a healthy node.

About Non-tiered Deployments

Services Gatekeeper can be deployed in a non-tiered deployment by using one of the following configurations:

- Multiple node configuration: A non-tiered, multiple node configuration is targeted toward smaller production environments that have less strict scalability and high availability requirements.
- Single node configuration: A non-tiered single node configuration is targeted toward test and development environments.

Service facades, service enablers, container services, and service interceptors are deployed in all nodes in non-tiered deployments.

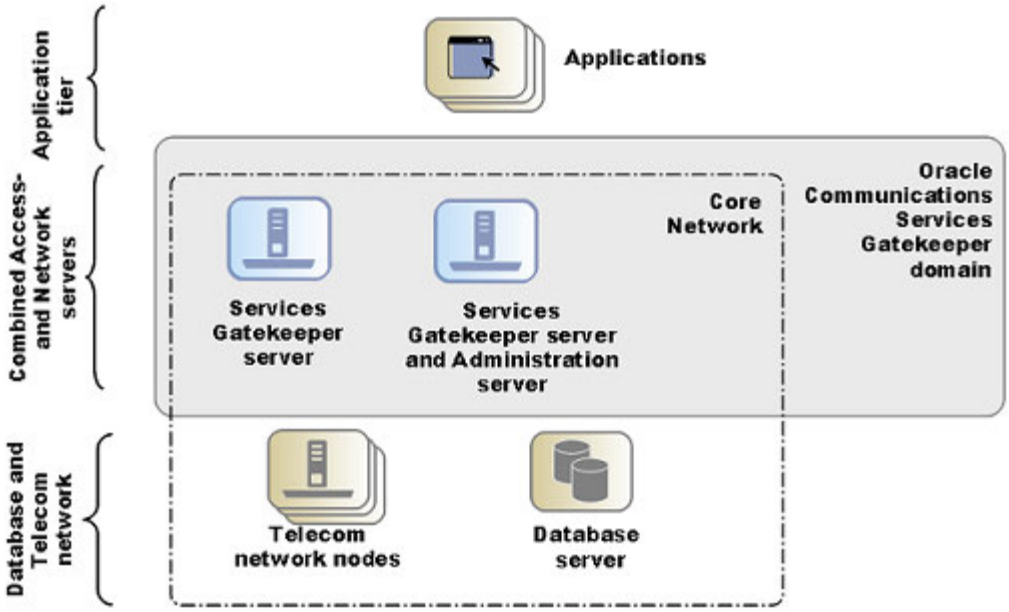
Using Non-tiered Deployments in Production Environments

You might use a non-tiered deployment in a production environment when security requirements and scalability requirements are irrelevant or minimal. An example of this is when Services Gatekeeper only serves applications hosted within the operators' domain and there is very restricted access to the IP network where Services Gatekeeper is deployed, and the integrity of the network is ensured by external mechanisms.

Scalability is compromised when you use a co-located access and Network Tier, because the individual servers cannot be optimized according to their diverse processing models.

Figure 2–5 shows a deployment that has a cluster configuration. The Administration Server also processes traffic. The cluster can contain two or more servers.

Figure 2–5 Example of a Dual Server Non-tiered Deployment for Basic High Availability

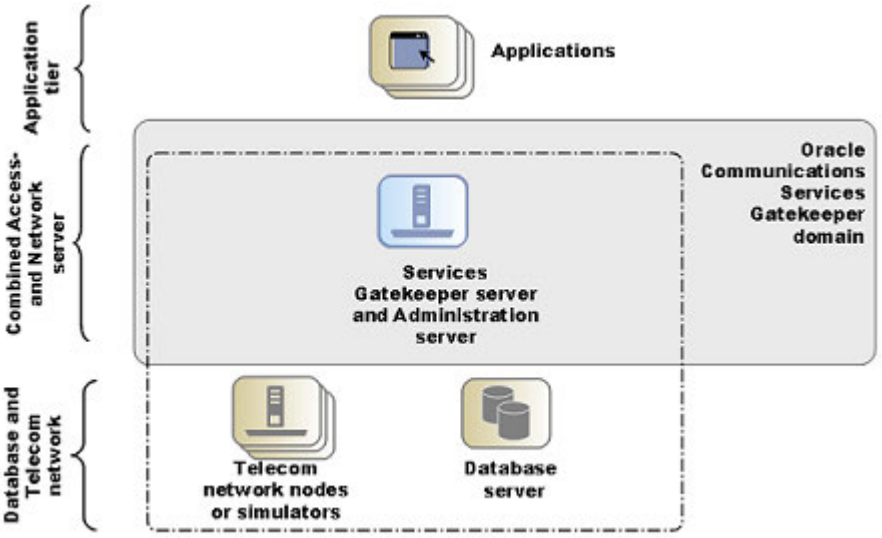


Using Non-tiered Deployments in Test and Development Environments

When you use Services Gatekeeper for functional testing of extensions and integrations, there is no immediate need for a multi-server configuration. A single-server configuration can be used to simplify management and configuration for the developer or tester.

Although it is possible to run several servers on a single physical machine, the only reason to do so is to run initial high availability tests. System tests should be performed on a deployment with multiple physical servers.

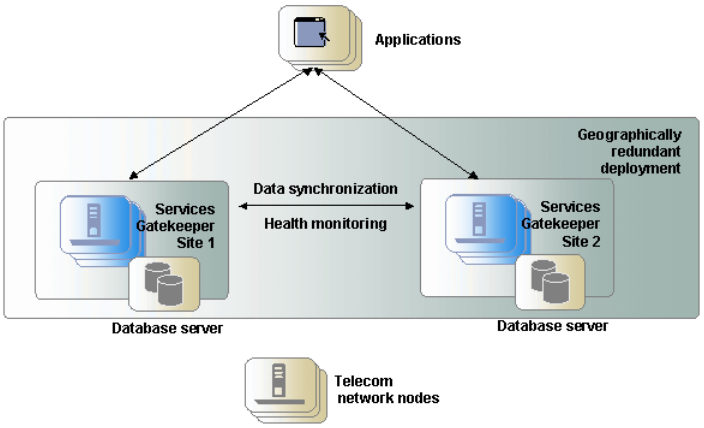
Figure 2–6 Example of a Single Node Non-tiered Deployment for Test and Development



About Geographically Redundant Deployments

Geographically separated deployments are important for high availability. To prevent service failure in the face of catastrophic events such as natural disasters or massive system outages caused by power failures, you can deploy Services Gatekeeper at two geographically distant sites that are designated as site pairs. As Figure 2–7 shows, each site, which is a Services Gatekeeper domain, has another site as its peer. Application and service provider configuration information, including related Service Level Agreements (SLAs) and budget information, is replicated and enforced across sites.

Figure 2–7 Example of a Geographically Redundant Deployment



Geographically redundant sites are the active-active type, which means that both sites in a pair can be used to process traffic simultaneously. These deployments are connected by communication channels for data synchronization and health monitoring. The data synchronization replicates budget information between the site pairs to enforce SLAs accurately. Applications should have site affinity, but have the ability to fail over to the other site if necessary. Each site is managed and configured independently. Accounts and SLAs are replicated across sites. Typically, one database tier is used per site.

All sites have a geographic site name and each site is configured to have a reference to its peer site using that name. The designated set of information is synchronized between these site peers.

One site is defined as the **geomaster**, the other as the **slave**. Checks are run periodically between the site pairs to verify data consistency and an alarm is triggered if mismatches are found, at which point the slave can be forced to synchronize to the geomaster. Any relevant configuration changes made to either site are written synchronously across the site pairs, so that a failure to write to one site causes the write to fail at the other site while triggering an alarm.

If a slave site becomes unavailable for any reason, the geomaster site becomes read-only, either until the slave site is available and has completed all data replication, or until the slave site has been removed from the geomaster site's configuration, terminating geographic redundancy. This behavior applies only to global configuration changes.

For applications, geographic redundancy means that their traffic can continue to flow in the event of a catastrophic failure at an operator site. Applications that normally use only a single site for their traffic can fail over to a peer site while maintaining ongoing

SLA enforcement for their accounts. This scenario is particularly relevant for SLA aspects that have longer term impact, such as quotas.

In many respects, the geographic redundancy mechanism is not transparent to applications. There is no single sign-on mechanism across sites, and an application must establish a session with each site it intends to use. In case of site failure, an application must manually fail over to a different site.

While application and service provider budget and configuration information are maintained across sites, state information for ongoing conversations is not maintained. Conversations in this sense are defined in terms of the correlation identifiers that are returned to the applications by Services Gatekeeper or passed into Services Gatekeeper from the applications. Any state associated with a correlation identifier exists on only a single geographic site and is lost if an entire site goes down. Conversational state includes, but is not limited to, call state and registration for network-triggered notifications. This type of state is considered volatile, or transient, and is not replicated at the site level.

As a result, conversations must be conducted and completed at their site of origin. If an application wants to maintain conversational state across sites, for example, to maintain a registration for network-triggered traffic, the application must register with each site individually.

About Domain Configuration Templates for Deployment Types

Services Gatekeeper ships with default domain configuration templates for each type of deployment that Services Gatekeeper supports. You use one of these templates to configure your domain. These templates contain the basic configurations for setting up domains, but you may need to adjust some aspects of the domain during the domain configuration process.

Table 2–2 summarizes the deployment templates.

Table 2–2 Domain Templates for Deployments

Domain Template Type	Template Name	Description
Basic developer configuration with co-located access and network tiers	**Basic Oracle Communications Services Gatekeeper Domain**	Creates an unified domain containing both the access and network tiers and the administration server all on a single machine. There is no support for high-availability configurations. The server does not belong to a cluster but is tied to the domain. This deployment type is common for non-production development machines where developers need access to Services Gatekeeper for functional testing of extensions and integrations.
Basic high-availability configuration	**OCSG Basic HA configuration**	Creates a basic high-availability, unified domain containing an access tier and network tier, each with two servers, and a database. One of the servers can also serve as the WebLogic administration server. The servers do not belong to a cluster but are tied to the domain. Database replication is not automatically provided and must be configured at the database level. This configuration can be expanded later. This deployment type is common for: ■ Non-production environments where developers need access to Services Gatekeeper for non-functional testing such as basic high-availability testing of extensions and integrations. ■ Basic, entry-level production environments that have limited requirements for security, because it does not support a DMZ separated by a firewall. It also provides minimal redundancy because it supports only two-server setups.
Access and network tier clusters	**OCSG Domain with Access and Network Clusters**	Creates a basic distributed domain, with a two-instance access tier cluster and a two-instance network tier cluster. A separate server has the role of the WebLogic administration server. This server does not process traffic requests. This configuration can be expanded later. High availability toward the database is not supported automatically. Redundancy toward the database is up to the database deployment. This deployment type is common for production environments and support deployments with a DMZ between the access and network tiers.
Access and network tier clusters with Oracle RAC database	**OCSG Domain with Access and Network Clusters with Oracle RAC Configuration**	Creates a basic distributed domain, with a two-instance access tier cluster and a two-instance network tier cluster. This configuration can be expanded later. It also creates the additional data sources required for use with an Oracle RAC-based installation. This configuration has all the properties of the access and network tier cluster setup and adds high availability and redundancy toward the database. This setup leverages the failover and redundancy characteristics of Oracle Real Application Cluster (Oracle RAC). This deployment type is common for production environments and supports deployments with a DMZ between the access and network tier.
Portal servers	**OCSG Portal Domain**	Creates a domain that contains the Portal server on a single machine.

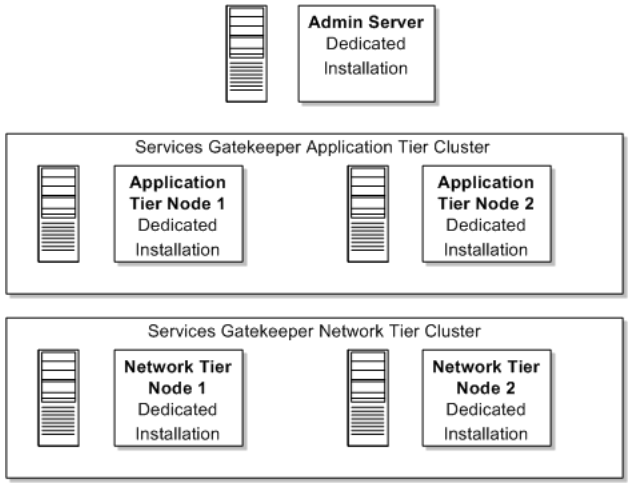
System Deployment Planning

All servers in a Services Gatekeeper cluster must be dedicated servers.

You must perform an installation on each machine in your Services Gatekeeper configuration.

Figure 2–8 shows a recommended Services Gatekeeper installation.

Figure 2–8 Recommended Services Gatekeeper Installation



See "Installing Services Gatekeeper" for detailed installation instructions.

About Setting Up Services Gatekeeper Reporting Support

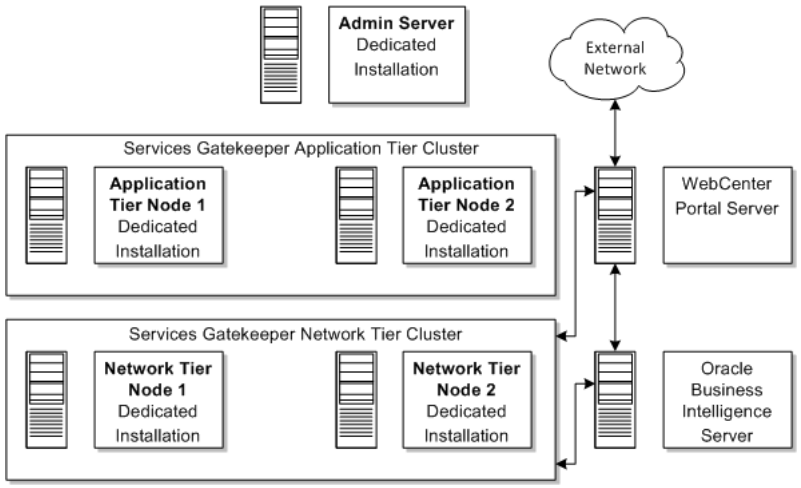
If you plan to install Services Gatekeeper reporting support, you will need additional servers to host Oracle Business Intelligence.

You install Services Gatekeeper reporting support by using a separate installer. Before you configure the reporting functionality, you must install and configure Oracle Business Intelligence, which prepares and renders the Services Gatekeeper reports.

Oracle Business Intelligence requires a dedicated server and an reports staging database.

Figure 2–9 shows a recommended Services Gatekeeper installation including a dedicated servers for Oracle Business Intelligence.

Figure 2–9 Recommended Services Gatekeeper Installation with Reporting



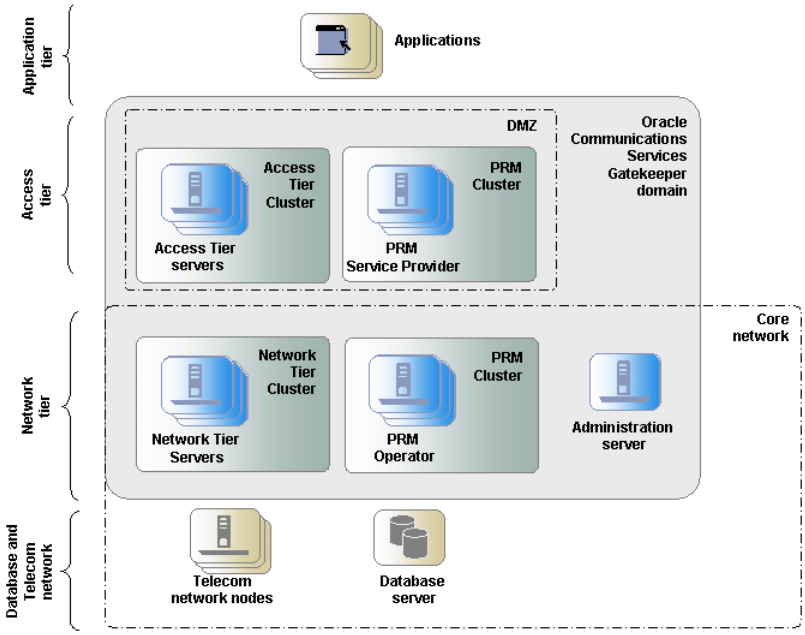
Note: A core Services Gatekeeper installation must be configured and running before you can install portal and reporting support.

About Deploying Partner Relationship Management Modules

Oracle recommends that you deploy the Partner Relationship Management (PRM) modules in a separate cluster in the domain. The PRM servers should not be co-located with Access Tier servers or Network Tier servers, because PRM processing impacts the performance of processing traffic requests.

There are two views to PRM: the service provider view and the operator view. Each view can be deployed separately. A portal application can benefit from being deployed in two parts: the service provider view deployed in the DMZ and the operator view deployed inside the secure network of the operator, not accessible from the Internet.

Figure 2–10 Example of a PRM Deployment



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 the section on RESTful services in *Services Gatekeeper Application Developer's Guide*.

About Enterprise Manager Compatibility

Services Gatekeeper is compatible with Oracle Enterprise Manager Cloud Control version 12*c*. For information about Enterprise Manager Cloud Control 12*c*, see the Enterprise Manager 12c page on the Oracle Technology Network website:

http://www.oracle.com/technetwork/oem/enterprise-manager/overview/index.html

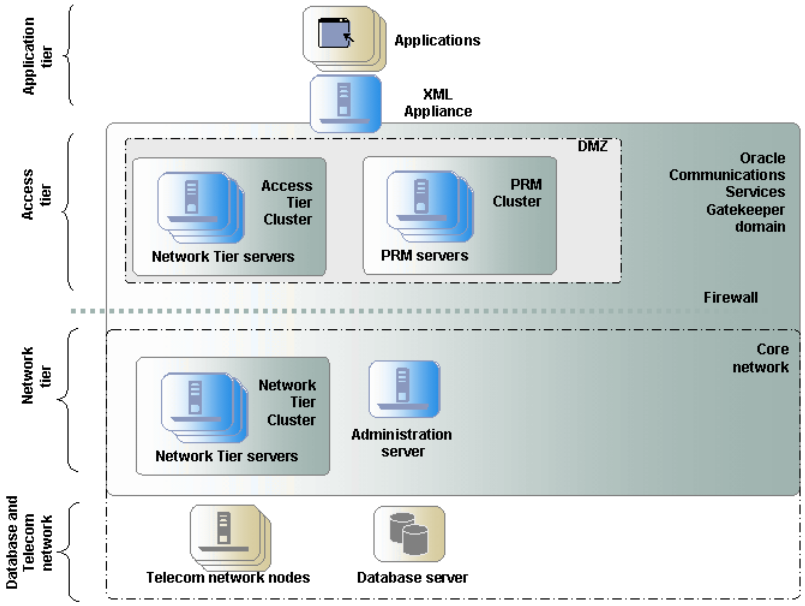
About XML Applications

Firewalls are required for a secure production deployment. See *Services Gatekeeper Security Guide* for a discussion of when to use firewalls.

XML appliances provide complement functionality provided by the Access Tier. They provide:

- XML acceleration using hardware in the form of ASIC circuits optimized for XML parsing, XPATH processing, and XSLT transformation and validation.
- Security applications, especially for:
  - XML screening for intrusion detection, traffic monitoring, and content filtering.
  - Firewall and Virtual Private Network applications for authentication, Web Services Security compliance and Single Sign-On.
  - Network gateway applications such as routing, traffic management, and protocol translation.

Figure 2–11 Example of a Deployment with XML Appliances



XML appliances in the form of firewalls are recommended in all deployments and are important between the Access Tier and the Internet. They facilitate setting up secure channels between applications and Services Gatekeeper.

XML Appliances do not provide high availability retries, health checks, or automatic synchronization of in-production upgrades.

The communication protocol between the access and Network Tiers is not XML. The Network Tier accepts and performs Java RMI calls.

Adding XML appliance in front of a Services Gatekeeper deployment adds another layer of latency.

Firewalls can be introduced between the Access Tier and the Network Tier. The tiered deployment model supported by Services Gatekeeper makes it very suitable for this.

To ensure network integrity, the Access Tier provides a set of carrier-grade security mechanisms that include:

- Web Services Security standards
- Message-level security, encryption, and trust
- Transport-level security
- Authentication, authorization and accounting (AAA)

All of these mechanisms are direct results of using WebLogic Server as a container. The authentication parts must be compliant with the account model used in Services Gatekeeper, unless double authentication procedures are performed, one procedure for the above and one for the Services Gatekeeper account.

For access control, Services Gatekeeper provides a set of enforcement rules, including time of day, day of week, and can take historical data into account. Examples of historical data are aggregated number of requests over a number of days or peak request rates expressed in milliseconds.

Services Gatekeeper deployments can benefit from the use of existing XML appliances, especially for the following use cases:

- Firewalls, both for fronting the deployment and for separating the access and Network Tier.
- Load balancers, to balance the load between servers in the access Tier.
- XML Schema validation (including message size, element size, and string lengths) for additional security and to off-load Services Gatekeeper message-validation processing.
- SSL termination points, to off-load the message-level and transport-level security processing from the Access Tier.

About Deployment Administration

All management, configuration, and provisioning operations at the Java EE level are performed using the Administration Server and are propagated to the relevant managed servers when the servers are deployed in clusters. Operations includes starting and stopping managed servers and deploying and undeploying Services Gatekeeper container services and communication services.

Container services and communication services using the Services Gatekeeper MBeans can be performed on any of the servers when the configured attribute is shared among all instances in the Network Tier cluster. When the configuration attribute is local for the server, the attribute must be configured on the individual server.

Services Gatekeeper components can be configured, managed, and provisioned by using a web-based administration GUI, interactive-text mode, scripting, and JMX.

For a complete list of Services Gatekeeper administration tasks and instructions, see *Services Gatekeeper System Administrator's Guide*.

Disk Storage Planning

You can use an ordinary disk system for disk storage. However, for performance and high availability reasons, a RAID system should be used.

Latency and Bandwidth Requirements

To avoid transaction processing issues related to latency or bandwidth restrictions Oracle provides the following guidelines for minimum latency and bandwidth requirements used in production environments.

Latency Requirements

Table 2–3 shows the minimum latency requirements between Services Gatekeeper entities in a production environment.

Table 2–3 Latency Guidelines for Services Gatekeeper Configurations

Configuration	Guideline
Network tier to database	Oracle recommends a latency value of less than 25 ms
Geo-redundant (site to site)	Oracle recommends a latency value of less than 1000 ms between sites

Bandwidth Requirements

Table 2–4 shows the minimum required bandwidth between Services Gatekeeper entities in a production environment. Bandwidth requirements depend on the traffic type and traffic load present in your environment. These guidelines are for typical deployments of Services Gatekeeper

Table 2–4 Bandwidth Guidelines for Services Gatekeeper Configurations

Configuration	Guideline
Network tier to database	At least 30 Mbps/1000 tps
Application tier to network tier	Less than 15ms
Geo-redundant (site to site)	At least 1 Mbps/1000 tps

Database Planning

The deployment architecture strongly favors deploying the database in a separate tier. The database should be deployed on dedicated servers for both security and performance reasons. Backup and other data-intensive operations should not increase load on traffic-processing servers. Database administrators should be granted exclusive privileges to log on and perform SQL operations. Configuration of Services Gatekeeper components should be performed by using the Services Gatekeeper management interfaces and should not be performed directly at the database level.

Oracle recommends that you use an Oracle database, where the instance is based on the transaction processing template, runs in dedicated server mode, and uses automatic store management.

3

Services Gatekeeper System Requirements

This chapter summarizes the system requirements for Oracle Communications Services Gatekeeper.

Software Requirements

Table 3–1 shows the Services Gatekeeper supported software. All values in the table apply to both the Access Tier and Network Tier.

Table 3–1 Oracle Communications Services Gatekeeper Supported Platform Matrix

OS Version	OS 32/64 Bit	Processor	JDK Version	JDK 32/64 Bit
Oracle Linux 4 (UL7+)	64	x64	JDK 1.7, plus the latest security updates	64
Oracle Linux 5 (UL3+)	64	x64	JDK 1.7, plus the latest security updates	64
Oracle Linux 6	64	x64	JDK 1.7, plus the latest security updates	64
Solaris 2.9 Update 9+	64	SPARC	JDK 1.7, plus the latest security updates	32 or 64
Solaris 10 Update 4+	64	SPARC	JDK 1.7, plus the latest security updates	32 or 64
Solaris 11	64	SPARC	JDK 1.7, plus the latest security updates	64
Red Hat EL 4 (UL7+)	64	x64	JDK 1.7, plus the latest security updates	64
Red Hat EL 5 (UL3+)	64	x64	JDK 1.7, plus the latest security updates	64
Red Hat EL 6 (UL3+)	64	x64	JDK 1.7, plus the latest security updates	64
Windows 7[1]	64	x64	JDK 1.7, plus the latest security updates	64

[1] Windows is only supported for use with development environments and is not recommended for production deployment.

Supported Databases

Table 3–2 shows the databases that Services Gatekeeper supports.

Table 3–2 Supported Databases

Database	Characteristic
Oracle 12*c* RAC	Full DB Failover and Fault Tolerance
Oracle 12*c* Single Instance	No Failover and Fault Tolerance
Oracle Database Express Edition 12*c*	No Failover and Fault Tolerance
Oracle 11*g* RAC	Full DB Failover and Fault Tolerance
Oracle 11*g* Single Instance	No Failover and Fault Tolerance
Oracle Database Express Edition 11*g*	No Failover and Fault Tolerance
MySQL Single Instance 5.6.14	No Failover or Fault Tolerance
MySQL Cluster 7.2.13	Full DB Failover and Fault Tolerance

Supported Virtualization Software

Services Gatekeeper is deployable and certified on Solaris Zones virtualized environment. For information about Solaris virtualization, see the Solaris overview on the Oracle Technology Network website:

http://www.oracle.com/us/products/servers-storage/solaris/virtualization-066073.html

Services Gatekeeper is also deployable and certified on Oracle VM. For information about Oracle virtualization, see the Oracle VM VirtualBox overview on the Oracle Technology Network website:

http://www.oracle.com/us/technologies/virtualization/oraclevm/061976.html

Supported Protocols

Services Gatekeeper supports the following protocols:

- Parlay X

  Services Gatekeeper supports Parlay X Version 2.1 and Parlay X Version 3.0. For details, see the descriptions of the individual communications service in *Services Gatekeeper Communication Service Reference Guide*.

- SNMP

  Services Gatekeeper supports SNMPv1 and SNMPv2.

- IPv6

  Services Gatekeeper is fully IPv6-compliant. It provides simultaneous IPv4/IPv6 support.

About Critical Patch Updates

Install all Oracle Critical Patch Updates as soon as possible. To download Critical Patch updates, find out about security alerts, and enable email notifications about Critical Patch Updates, see the "Security" topic on the Oracle Technology Network website:

http://www.oracle.com/technetwork/topics/security/whatsnew/index.html

Hardware Requirements

Services Gatekeeper requires the following hardware:

- For the Services Gatekeeper software:
  - RAM: 1 GB required; 2 GB recommended
  - Disk space: 2 x 36 GB
- For the database:
  - RAM: 2 GB required; 6 GB recommended
  - Disk space: 2 x 36 GB

There must be at least 1.5 GB of disk space available under **/usr/local**.

Information Requirements

Table 3–3 shows the information you must provide during the Services Gatekeeper installation.

Table 3–3 Required Information

Information Type	Description	Default Value
Host name or IP address	The network names or IP addresses of the machines on which you are going to install the software.	Current host name or IP address
Directory	The directory on each machine that will serve as your *Middleware_home* directory.	NA
Directory	The directories on each machine in which to install Services Gatekeeper and WebLogic Server software. By default, these are subdirectories of *Middleware_home*.	NA
Directory	If you are going to install Services Gatekeeper Platform Development Studio, the Eclipse plug-in directory.	NA
Password	A password for the administrative user. The password must have a minimum of eight characters, at least one of which is non-alphabetic.	NA

4

Installing the Database

This chapter provides an overview of installing a supported database for use with Oracle Communications Services Gatekeeper.

Database Installation Overview

Although there are substantial differences between the installation procedures for each type of database, all installation types include the following basic steps:

1. Installing the database software.
2. Setting up a user account that Services Gatekeeper uses to access the database.
3. Granting the user account appropriate privileges on the database.

See the following sections for information about the database you are installing:

- Installing Oracle RAC or Oracle Single Instance Database Software
- Installing Oracle Database Express Edition
- Installing MySQL Database
- Installing MySQL Cluster CGE

Installing Oracle RAC or Oracle Single Instance Database Software

Follow these instructions if you are using Oracle Real Application Clusters (Oracle RAC) or Oracle Database Single Instance database software.

The database must be installed on a dedicated server running outside the Services Gatekeeper cluster.

About Using Oracle RAC with WebLogic Server

Oracle RAC or MySQL are supported production environments that require high availability.

For information about using Oracle WebLogic Server with multiple data sources, see *Oracle Fusion Middleware Administering JDBC Data Sources for Oracle WebLogic Server*.

Installing the Database Software

To install the database software:

1. Follow the instructions in the database installation guide, available in the installing and upgrading section on the *Oracle Database Documentation Library* website.

During the installation process, select these configuration options:

- Create the database using the **Transaction Processing** template.
- Use the **Dedicated Server Mode** for the database.
- Change the **processes** parameter to be equal to:

  [(`wlng.datasource MaximumCapacity + wlng.localTX.datasource MaximumCapacity`) * *NumberOfServers*]

  where *NumberOfServers* is the number of Services Gatekeeper servers in the cluster. **MaximumCapacity** is a parameter in the connection pool settings for the JDBC data sources. Normally this value is 150 for both data sources, but you may need to increase it.

2. Download and install the latest Oracle database patch set.
3. Continue to "Setting Up a Services Gatekeeper User for the Oracle Database".

Setting Up a Services Gatekeeper User for the Oracle Database

To set up a Services Gatekeeper user for the Oracle database:

1. Create a database user for Services Gatekeeper with an allowed (unlimited) quota on its default tablespace (the **users** tablespace). The user name and password for the user are later copied to each Services Gatekeeper server.
2. Grant the user the following privileges:
   - CREATE SESSION
   - CREATE TABLE
3. Continue to "Installing Services Gatekeeper".

Installing Oracle Database Express Edition

Follow the instructions in this section if you are using Oracle Express Edition (XE) as your database.

Oracle XE can be installed either on a server in the Services Gatekeeper cluster or on a separate server. If it is installed in the cluster, it should be in the same server as the Network Tier.

> **Note:** Oracle XE is recommended over MySQL for Services Gatekeeper development installations because the Oracle XE schema is compatible with enterprise Oracle databases. Neither Oracle XE nor MySQL is recommended for production deployment.

Installing the Oracle XE Software

To install Oracle XE:

1. Download the Oracle Database Express Edition installer from the Oracle Technology Network website:

   `http://www.oracle.com/technetwork/index.html`

2. Follow the instructions to select and download the Oracle Database Express Edition software for your operating system.

3. Install Oracle XE using the instructions in the installation guide on the Oracle documentation website at:

   https://docs.oracle.com/en/database/

4. Continue to "Configuring Oracle XE for Services Gatekeeper".

Configuring Oracle XE for Services Gatekeeper

To configure Oracle XE for Services Gatekeeper:

1. Open a command window.
2. (Linux only) If the required environment variables are not already set, do the following:

   For Bash, Bourne, or Korn shell, enter the following command:

   ```
   source ORACLE_HOME/bin/oracle_env.sh
   ```

   For C shell, enter the following command:

   ```
   source ORACLE_HOME/bin/oracle_env.csh
   ```

3. Enter the following command:

   ```
   sqlplus /nolog
   ```

4. Connect to the database (on Windows you are prompted for the user name and password):

   ```
   SQL> connect SYSTEM/SYSTEM_user_password@XE
   ```

5. Enter the following command to increase the number of allowable JDBC connections:

   ```
   SQL> alter system set processes=300 scope=spfile;
   ```

6. Create a Services Gatekeeper user and password using the following command:

   ```
   SQL> create user database_username identified by password;
   ```

7. Grant the newly created user privileges using the following command:

   ```
   SQL> grant create session, create table, resource to database_username;
   ```

8. Exit SQL*Plus:

   ```
   SQL> exit
   ```

9. Restart the database for the changes to take effect.
10. Continue to "Installing Services Gatekeeper".

Installing MySQL Database

Follow the instructions in this section if you are using MySQL as your database. Services Gatekeeper supports using single instance and clustered MySQL database implementations.

MySQL can be installed either on a server in the Services Gatekeeper cluster or on a separate server. If it is installed in the cluster, it should be in the same server as the Network Tier.

Note: Oracle XE is preferable to MySQL for Services Gatekeeper development installations because the Oracle XE schema is compatible with enterprise Oracle databases. Oracle XE is not recommended for production deployment.

This section covers the following topics:

- Installing the MySQL Database Software
- Configuring MySQL on Linux
- Configuring MySQL on Windows
- Creating the Database and a Database User

Installing the MySQL Database Software

To install a MySQL database:

1. Download the MySQL database software from the Oracle software delivery website at:

   `https://edelivery.oracle.com`

2. Follow the instructions in the MySQL documentation for installing MySQL. The documentation is available on the MySQL website at:

   `http://dev.mysql.com`

3. When installing MySQL:
   - **Linux**: For most Linux distributions, you can use a package manager such as **dpkg** or YUM.
   - **Windows**: Unless you have additional special requirements, you can select the **Developer Default** installation option.
4. Continue to one of the following sections:
   - Configuring MySQL on Linux
   - Configuring MySQL on Windows

Configuring MySQL on Linux

This section summarizes the commands required to configure MySQL on most versions of Linux. Command locations may differ between Linux distributions.

To configure MySQL on Linux:

1. As the user root, start the MySQL database:

   ```
   /etc/rc.d/init.d/mysqld start
   ```

2. Open the **/etc/my.cnf** file and do the following:
   - Edit the connection variable so that **max_connections** is equal to:

     [(`wlng.datasource MaximumCapacity + wlng.localTX.datasource MaximumCapacity`) * *NumberOfServers*]

     where *NumberOfServers* is the number of Services Gatekeeper servers in the cluster. **MaximumCapacity** is a parameter in the connection pool settings for

the JDBC data sources. Normally this value is 150 for both data sources, but you may need to increase it.

```
[mysqld]
max_connections=400
```

- Add an entry for the default character set. The recommended character set is **Latin1**.

```
default-character-set=latin1
```

3. Save and close the file.
4. Restart MySQL:

```
/etc/rc.d/init.d/mysqld stop
/etc/rc.d/init.d/mysqld start
```

5. Continue to "Creating the Database and a Database User".

Configuring MySQL on Windows

To configure MySQL on Windows:

1. From a text editor, open the **my.ini** file and do the following:
   - Edit the connection variable so that **max_connections** is equal to:

     [(`wlng.datasource MaximumCapacity + wlng.localTX.datasource MaximumCapacity`) * *NumberOfServers*]

     where *NumberOfServers* is the number of Services Gatekeeper servers in the cluster. **MaximumCapacity** is a parameter in the connection pool settings for the JDBC data sources. Normally this value is 150 for both data sources, but you may need to increase it.

     ```
     [mysqld]
     max_connections=400
     ```

   - Add an entry for the default character set. The recommended character set is **Latin1**.

     ```
     default-character-set=latin1
     ```

2. Save and close the file.
3. Continue to "Creating the Database and a Database User".

Creating the Database and a Database User

To configure MySQL for Services Gatekeeper, perform the following for each IP address in the cluster:

1. Create the Services Gatekeeper database user and password.

   You will need to provide this user name and password when you configure the Services Gatekeeper domain. For information about the various command-level modes of accessing the MySQL server, see the documentation on the MySQL website.

2. Grant access privileges:

   ```
   GRANT ALL ON *.* TO database_username@ip_address IDENTIFIED BY user_password
   ```

3. Create the database for Services Gatekeeper:

   ```
   CREATE DATABASE database_name
   ```

   You will need to provide the database name when you configure the Services Gatekeeper domain.

4. Continue to "Installing Services Gatekeeper".

Installing MySQL Cluster CGE

Follow the instructions in this section if you are using MySQL Cluster Carrier Grade Edition (CGE) as your database. Services Gatekeeper supports using single instance and clustered MySQL database implementations.

MySQL can be installed either on a server in the Services Gatekeeper cluster or on a separate server. If it is installed in the cluster, it should be in the same server as the Network Tier.

Installing the MySQL Cluster CGE Software

To install MySQL Cluster SGE software:

1. Download a supported version of MySQL Cluster from the Oracle software delivery website:

   https://edelivery.oracle.com/

2. Install the MySQL Cluster CGE software using the instructions in the installation guide on the Oracle documentation website:

   http://docs.oracle.com/cd/E17952_01/index.html

Configuring the Management Server Node

For a first Cluster, start with a single MySQL Server (mysqld), a pair of Data Nodes (ndbd) and a single management node(ndb_mgmd) – all running on the same server. Using the management server node, you can start and stop other nodes, configure data, run backup, and perform other tasks.

To configure the management server node:

1. Create the **config.ini** file on the management server, under the **/var/lib/mysql-cluster/** directory.

   The following is an example of the **ndbd default** section in the **config.ini** file. For the **hostname** parameter, *host_name_or_IP_address* represents the host name or IP address of the node. For example:

   hostname=node1.example.com

   The system values in this example are suggested values. The values you use will depend on how your system is set up.

   Example **ndbd default** section of the **config.ini** file:

   ```
   [ndbd default]
   NoOfReplicas=2
   DataMemory=4G
   IndexMemory=400M
   MaxNoOfAttributes=500000
   MaxNoOfTables=1760
   MaxNoOfOrderedIndexes=3000
   ```

```
MaxNoOfUniqueHashIndexes=1250
MaxNoOfConcurrentOperations=100000
[ndb_mgmd]
NodeId=1
hostname=host_name_or_IP_address
datadir=/var/lib/mysql-cluster/
[ndbd]
NodeId=2
hostname=host_name_or_IP_address
datadir=/usr/local/mysql/data/
[ndbd]
NodeId=3
hostname=host_name_or_IP_address
datadir=/usr/local/mysql/data/
[mysqld]
NodeId=4
hostname=host_name_or_IP_address
[mysqld]
NodeId=5
hostname=host_name_or_IP_address
[mysqld]
[mysqld]
```

2. Create the **my.cnf** file under the **/etc** directory, using the following values:

```
[mysqld]
ndbcluster
datadir=/usr/local/mysql/data
basedir=/usr/local/mysql
user = mysql
port = 3306
default-storage-engine=ndb
ndb-connectstring= host_name_or_IP_address
[mysql_cluster]
ndb-connectstring= host_name_or_IP_address
```

Starting the MySQL Cluster Processes

To start the MySQL Cluster processes:

1. Enter the following commands in order:

```
./ndb_mgmd -f /var/lib/mysql-cluster/config.ini
./ndbd
mysqld_safe--ndb_nodeid=4 --user=mysql&
```

After you run these commands, the **ndb_mgm** prompt appears.

2. Check the status of the cluster by entering the following command:

```
ndb_mgm> show
```

The status of the cluster is displayed on the command line. For example:

```
Connected to Management Server at: 12.345.67.81:1186
Cluster Configuration
---------------------
[ndbd(NDB)]     2 node(s)
id=2    @12.345.67.82  (mysql-5.5.30 ndb-7.2.12, Nodegroup: 0, Master)
id=3    @12.345.67.83  (mysql-5.5.30 ndb-7.2.12, Nodegroup: 1)

[ndb_mgmd(MGM)] 1 node(s)
```

```
id=1    @12.345.67.82  (mysql-5.5.30 ndb-7.2.12)

[mysqld(API)]   3 node(s)
id=4    @12.345.67.82  (mysql-5.5.30 ndb-7.2.12)
id=5    @12.345.67.83  (mysql-5.5.30 ndb-7.2.12)
id=6 (not connected, accepting connect from any host)
```

Wait for the data nodes to finish starting.

3. Start your MySQL server.

5

Installing Services Gatekeeper

This chapter describes how to install Oracle Communications Services Gatekeeper.

Before installing Services Gatekeeper, read these chapters:

- Services Gatekeeper Installation Overview
- Planning Your Services Gatekeeper Installation
- Services Gatekeeper System Requirements

About Installing Services Gatekeeper

You must install Services Gatekeeper on every server in your implementation. You must install the software in a directory that resides on the server's local file system.

You install Services Gatekeeper by using a generic installer that works on any supported operating system and for both 64-bit and 32-bit platforms.

Installation Prerequisites

The generic installer does not include a bundled JDK. The JDK must already be installed when you use the generic installer.

Installing the JDK

You must download and install a supported JDK on the target system before installing Services Gatekeeper. If you are installing on a 64-bit system, you must install a 64-bit JDK or a hybrid 32/64-bit JDK. See "Software Requirements" for information about the required JDK version.

Download the JDK from the Java page on the Oracle Technology Network website at:

`http://www.oracle.com/technetwork/java/index.html`

Setting the Java Path

To ensure that the appropriate JDK is installed and that the Java path is set:

1. Log in to the target system.
2. Run the `java -version` command, or `java -d64 -version` command on platforms using a 32/64-bit hybrid JDK, to ensure that the **JAVA_HOME** variable is set to a 64-bit JDK.

   If JAVA_HOME is not correctly set, set it to point to the correct JDK.

3. Add the **bin** directory of the JDK that you installed to the beginning of the **PATH** variable definition. For example:

```
PATH=$JAVA_HOME/bin:$PATH
export PATH
```

Where JAVA_HOME represents the full path to the JDK directory.

Creating an Installation Log

To create an installation log, add the following option to any of the commands that launch the installer:

-log=*logfilename*

where *logfilename* is a name that you assign to the log file.

For example, the following command runs the installer in GUI mode and creates a log file named **install_log** containing the installation's output.

```
java -jar ocsg_multitier_generic.jar -log=install_log
```

Installing Services Gatekeeper in GUI Mode

This section describes how to install Services Gatekeeper in GUI mode.

Important:

- Installing Services Gatekeeper on Windows is supported only for development and test environments; it is not supported for production.
- If you are installing on Windows, you must log in as an administrator.
- After starting the installer, you can cancel the installation at any time by clicking **Exit**.

To install Services Gatekeeper in GUI mode:

1. Log in to the target system.
2. Download the Services Gatekeeper installer from the Oracle software delivery website:

   https://edelivery.oracle.com/

3. Change to the directory where you downloaded the software.
4. Start the installer.
   - To start the installer on a system that uses a 32/64-bit hybrid JDK, enter:

     ```
     java -d64 -jar ocsg_multitier_generic.jar [-log=logfilename]
     ```

   - To start the installer on a 32-bit system, enter:

     ```
     java -jar ocsg_multitier_generic.jar [-log=logfilename]
     ```

   After the installer starts, the Welcome screen appears.
5. Click **Next**.

The Installation Location screen appears.

6. In the **Oracle Home** field, enter the full path to the directory of your *Middleware_home* or use the **Browse** button to locate the directory.

   The *Middleware_home* directory is the central directory for all Oracle products installed on the target system.

   To see a list of Services Gatekeeper products that are currently installed in the directory, click **View**.

7. Click **Next**.

   The Installation Type screen appears.

8. Specify the components to install on this system by doing one of the following:

   - To install only the Administration Server, select **Administration Server** and click **Next**.
   - To install only the Network Tier, select **Network Tier** and click **Next**.
   - To install only the Portal server:

     a. Select **Portal** and click **Next**.

        The Portal Parameters screen appears.

     b. In the **Access Tier Servers** field, enter the address for each Access Tier server in your Services Gatekeeper implementation. The address uses the format *IPAddress*:*Port*. Each address must appear on its own line.

        The IP address and port of the backend server must match the IP address and port of the Access Tier. To view the Access Tier server port, in the Administration Console, click **Servers**, then **AT Server Name**, and then **Listen Port**.

     c. Click **Next**.

   - To install only the Access Tier, select **Access Tier** and click **Next**.
   - To install multiple Services Gatekeeper components:

     a. Select **Custom Installation** and click **Next**.

        The Features to Install screen appears.

     b. Select the checkbox for each component that you want to install on this system. To install all of the components, select the **Oracle Communication Services Gatekeeper** checkbox.

     c. Click **Next**.

   The Prerequisite Checks screen appears.

9. The screen automatically tests your system to ensure that it meets all operating system and JDK software requirements:

   - A green check mark indicates that your system passed the prerequisite check.
   - A red circle indicates a problem. The bottom of the screen shows a short error message to help you troubleshoot the problem. Fix the error and click **Rerun** to perform the prerequisite checks again. To continue the installation without fixing the problem, click **Skip**.

10. Click **Next**.

    The Installation Summary screen appears.

11. Ensure that the listed installation location and feature sets to install are correct.

    If the list is not correct, you can use the **Back** button to make corrections.

    To save the information to a response file so you can install the component later, click **Save Response File** and specify the name and location of the response file.

12. Click **Install** to start the installation.

    The Installation Progress screen appears, and a progress bar indicates the status of the installation process.

13. Click **Next**.

14. When the Installation Complete screen appears, do one of the following:

    Important: If you plan to use Services Gatekeeper with an IPv6 network, do not configure the domain now. You must perform certain post-installation tasks first.

    - To configure your Services Gatekeeper domain now, click **Finish**.

      The WebLogic Server Configuration Wizard starts.

    - To complete installation without configuring your domain, deselect **Automatically Launch the Configuration Wizard** and click **Finish**.

      The Services Gatekeeper installer exits.

After installation completes, the WebLogic Server Configuration Wizard starts by default. For information about how to configure your Services Gatekeeper domain, see "Configuring the Domain in GUI Mode".

Installing Services Gatekeeper in Silent Mode

Silent mode is a way of setting installation options once and then using those settings to duplicate the installation on many machines. The installation program reads your settings from a Response File that you create prior to beginning the installation. The installation program does not display any options during the installation process. Silent-mode installation works on Windows, Solaris, and Linux systems.

About the Response File

The entries in the Response File (**response.rsp**) correspond to the prompts that you would see if you used GUI mode.

Incorrect entries in the Response File can cause the installation to fail. To help you determine the cause of a failure, Oracle recommends that you create a log file when you start the installation.

The following is a sample version of the Response File. Your input may be slightly different, depending on your installation.

```
[ENGINE]

#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

#The Oracle home location. This can be an existing Oracle Home or a new Oracle
```

```
Home.
ORACLE_HOME=c:\oracle\ocsg6.0

#Set this variable value to the Installation Type selected (for example, WebLogic
Server, Coherence, Complete with Examples).
INSTALL_TYPE=Complete with Examples

#Provide the My Oracle Support Username. If you want to ignore Oracle
Configuration Manager configuration, provide an empty string
#for the user name.
MYORACLESUPPORT_USERNAME=

#Provide the My Oracle Support Password
MYORACLESUPPORT_PASSWORD=<SECURE VALUE>

#Set this to true if you want to decline the security updates. Setting this to
true and providing an empty string for the My Oracle Support
#username will ignore the Oracle Configuration Manager configuration.
DECLINE_SECURITY_UPDATES=true

#Set this to true if My Oracle Support Password is specified.
SECURITY_UPDATES_VIA_MYORACLESUPPORT=false

#Provide the Proxy Host.
PROXY_HOST=

#Provide the Proxy Port.
PROXY_PORT=

#Provide the Proxy Username.
PROXY_USER=

#Provide the Proxy Password.
PROXY_PWD=<SECURE VALUE>

#Type String (URL format) Indicates the OCM Repeater URL which should be of the
format [scheme[Http/Https]]://[repeater host]:[repeater port]
COLLECTOR_SUPPORTHUB_URL=
```

Returning Exit Codes to the Console

When run in silent mode, the installation program generates exit codes that indicate the success or failure of the installation. Table 5–1 describes these exit codes:

Table 5–1 Installation Program Exit Codes

Code	Description
0	Installation completed successfully.
-1	Installation failed due to a fatal error.
-2	Installation failed due to an internal XML parsing error.

When you start the silent-mode installation process from a script, you can use the **echo** command to have these exit codes displayed to the console. The following is a sample command file that invokes the installer in silent mode and sends the exit codes to the console.

Example 5–1 Script that Returns Exit Codes

```
rem Execute the installer in silent mode
@echo off
java -jar ocsg_multitier_generic.jar -silent
-responseFile=/home/use/bin/response.rsp -log=logfilename

@rem Return an exit code to indicate success or failure of installation
set exit_code=%ERRORLEVEL%

@echo.
@echo Exitcode=%exit_code%
@echo.
@echo Exit Code Key
@echo ---------------
@echo  0=Installation completed successfully
@echo -1=Installation failed due to a fatal error
@echo -2=Installation failed due to an internal XML parsing error
@echo.
```

Running the Installer in Silent Mode

To install Services Gatekeeper in silent mode on any supported platform:

1. Log in to the target system.
2. Download the Services Gatekeeper installer from the Oracle software delivery website:

   https://edelivery.oracle.com/

3. Create a **response.rsp** file, as described in "About the Response File".
4. Change to the directory where you downloaded the software.
5. Start the installer by entering the following command:

   ```
   java -jar ocsg_multitier_generic.jar -silent -responseFile ResponseFile
   ```

   where *ResponseFile* is the full path and name of the Response File. For example, **/home/use/bin/response.rsp**.

6. Check whether the installer completed successfully by retrieving the exit codes, as described in "Returning Exit Codes to the Console".

Where to Go from Here

If you want to install:

- Services Gatekeeper Reports, see "Installing Services Gatekeeper Reports".
- Services Gatekeeper Platform Test Environment (PTE), see "Installing the Platform Test Environment".
- Services Gatekeeper Application Test Environment (ATE), see "Installing the Application Test Environment".

Otherwise, perform the tasks in "Services Gatekeeper Post-Installation Tasks".

6

Services Gatekeeper Post-Installation Tasks

This chapter provides instructions for Oracle Communications Services Gatekeeper post-installation tasks. You must install Services Gatekeeper before following these procedures. See "Installing Services Gatekeeper".

Overview of Services Gatekeeper Post-Installation Tasks

After installing Services Gatekeeper, you perform the following tasks:

1. Set the WebLogic Server home path.
2. Configure the Services Gatekeeper domain.
3. Perform post-installation tasks for the Services Gatekeeper installation.
4. Perform post-installation tasks for any optional components that you installed, which may include:
   - Services Gatekeeper Reports
   - Services Gatekeeper Platform Test Environment
   - Services Gatekeeper Application Test Environment

Setting the WebLogic Server Home Path

To set the WebLogic Server home path:

1. Set the WL_HOME variable to the directory in which you installed the WebLogic Server software. For example:

   ```
   WL_HOME=Middleware_home/wlserver
   ```

2. Export WL_HOME. For example:

   ```
   export WL_HOME
   ```

Configuring Your Services Gatekeeper Domain

In order to run Services Gatekeeper, its container (Oracle WebLogic Server) must be given basic information about the various parts of the system. This is called configuring the domain.

You configure the domain by running the WebLogic Server Configuration Wizard or by using the WebLogic Scripting Tool (WLST). For instructions, see "Configuring the Services Gatekeeper Domain".

Post-Installation Tasks for Services Gatekeeper

Perform these tasks on systems where you installed Services Gatekeeper.

Creating JMS Servers for Additional Network Tier Servers

If you added Network Tier servers in addition to the initial two provided by the default clustered domain templates, you must configure Services Gatekeeper to add support for the EDR Service on each server. Each server in the Network Tier requires its own JMS server in order for the EDR Service to work correctly.

For the following task, you must start the administrative server in your Services Gatekeeper installation so that you can use the Administration Console to make the necessary adjustments. Unless you are setting up an all in one domain, you also need to start at least one Network Tier server (this prevents a null pointer error when initializing the Administration Console). For more information about using the Administration Console, see *Services Gatekeeper System Administrator's Guide*.

To create the required JMS servers:

1. Start the Administration Server.
2. In a command window, go to the **domain/bin** directory.

   In the default installation, this would be *Middleware_home***/user_projects/domains/base-domain/bin**.
3. Run the following command:
   - Linux/Solaris:

     ```
     sh startWebLogic.sh
     ```
   - Windows:

     ```
     startWebLogic.cmd
     ```

   The Administration Server starts and displays output in the command window. Wait until the prompt indicates that the server is in **RUNNING** state.

   Note: This script works best with the Bash shell. If the server fails to start and returns this error:

   ```
   ./dbController.sh: 3: -/dbController.sh: Syntax Error: "(" unexpected
   ```

   edit the **startWeblogic.sh** script, changing the **#!/bin/sh** shebang to **#!/bin/bash**.

   ---
4. If you are setting up an all-in-one domain, skip this step. Otherwise, do the following:
   a. (Solaris only) Add the following line to the *Middleware_home***/user_projects/domains/base-domain/bin/startManagedWebLogic.sh** script:

      ```
      JAVA_OPTIONS="${JAVA_OPTIONS} -Dweblogic.ThreadPoolSize=100
      -Dweblogic.ThreadPoolPercentSocketReaders=50"
      ```
   b. Save and close the file.
   c. Start a Network Tier server by doing one of the following:

- **Run the start script from the network tier server:** Log in to the Network Tier server and run the **startManagedWebLogic.sh** script.
- **Run the start script from the domain/bin directory:** In a separate command window, go to *Middleware_home*/**user_projects/domains/base-domain/bin** and enter the following command:

  ```
  sh startManagedWebLogic.sh network_node t3://admin_host:port
  ```

  where *network_node* is the name of the Network Tier server, and *admin_host* and *port* are the host name and port number of the Administration Server.

Watch the command window as the Network Tier server loads. Wait until the prompt indicates that the server is in **RUNNING** state.

5. When both servers are in **RUNNING** state, start the Administration Console.

   In your browser, enter the following address:

   ```
   http://hostname:port/console
   ```

   where *hostname* is the host name of the Administration Server, and *port* is the port number used for the listen address assigned during domain configuration.

6. Log in using your login credentials.

   If this is the first time you have logged in, you should use username: `weblogic` and a password that you create. There are instructions in *Services Gatekeeper System Administrator's Guide* on changing these values after your system is fully configured.

7. Click **Lock & Edit** in **Change Center**.

8. Create the new JMS server:

   a. In the Administration Console, select **Home**, then **Services**, then **Messaging**, and then **JMS Servers**.

   b. Click **New**.

   c. In the **Name** field, enter the name of the JMS Server.

   d. From the **Target** menu, select the Network Tier server on which to create the JMS server.

   e. Click **Finish**.

   f. Click **Activate Changes**.

(Optional) Adding a Custom Password Validator

You can add a custom password validator to Services Gatekeeper by using features available through Oracle WebLogic Server. To do so, you create and configure a **Password Validation Provider**. This allows you to enforce rules concerning the composition of passwords used with Services Gatekeeper. In general, the rules include:

- Whether the password may contain the user's name, or the reverse of that name
- A minimum or maximum password length (composition rules may specify both a minimum and maximum length)
- Whether and how many of the following characters must be in the password:
  - Numeric characters
  - Lowercase alphabetic characters

- Uppercase alphabetic characters
- Non-alphanumeric characters (for example, parentheses or asterisks)

For more information about adding password validation to your Services Gatekeeper installation, see "Configuring the Password Validation Provider" in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

(Optional) Adding Java Cryptography Extensions

Services Gatekeeper does not require Java Cryptography Extensions (JCE) features to run, but you can install them if your implementation requires them. For more information about adding JCE, see "Using JCE Providers with WebLogic Server" in *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

Post-Installation Tasks for Reports

Perform these tasks if you installed Services Gatekeeper Reports as described in "Installing Services Gatekeeper Reports".

Configuring the Reports Data Source

Before you begin, make sure you have the following information for your reports database.

- Database Name
- Host Name
- Database Server Port
- Database User Name
- Database User's Password

To configure the reports staging data source:

1. Make sure that the Services Gatekeeper Administration Server is running.
2. Start the Administration Console by entering the following URL in your web browser:

   `http://hostname:port/console`

   Where *hostname* is the DNS name or IP address of the Services Gatekeeper Administration Server and *port* is the address of the port on which the Administration Server is listening for requests (8001 by default).
3. When the login page appears, enter the user name and the password you used to start the Administration Server (you may have specified this user name and password during the Services Gatekeeper installation process), or enter a user name that has been granted one of the default global security roles.
4. In the Change Center of the Administration Console, click **Lock & Edit**.
5. In the **Domain Structure** tree, select your Services Gatekeeper domain and expand **Services**, then **JDBC**, and then select **Data Sources**.
6. On the Summary of Data Sources page, click **New** and choose **Generic Data Source** from the list.
7. On the JDBC Data Sources Properties page, specify the following information:

- **Name**: Enter the following name for the JDBC data source: **analytic.datasource**
- **JNDI Name**: Enter the following path to the JDBC data source: **oracle.ocsg.edr.analytic**
- **Database Type**: Select the DBMS type of the database you're using as your reports staging database. If your DBMS is not listed, select Other.

Click **Next** to continue.

8. Select the JDBC driver you want to use to connect to the database.

   Note: You must install JDBC drivers before you can use them to create database connections. Some JDBC drivers are installed with WebLogic Server, but many are not installed.

   Click **Next** to continue.

9. On the Connection Properties page, enter values for the following properties:
   - **Database Name**: Enter the name of your reports database.
   - **Host Name**: Enter the DNS name or IP address of the server hosting the reports database.
   - **Port**: Enter the port on which the database server listens for connections requests.
   - **Database User Name**: Enter the reports database username.
   - **Password/Confirm Password**: Enter the password for the reports database user.

   Click **Next** to continue.

10. On the Test Database Connection page, review the connection parameters and click **Test Configuration**.

    Services Gatekeeper attempts to create a connection from the Administration Server to the database. Results from the connection test are displayed at the top of the page. If the test is unsuccessful, you should correct any configuration errors and retry the test.

11. Click **Next** to continue.
12. On the Select Targets page, select all of your Services Gatekeeper Network Tier servers or clusters.
13. Click **Finish** to save the JDBC data source configuration and deploy the data source to the targets that you selected.
14. To activate your changes, in the **Change Center** of the Administration Console, click **Activate Changes**.

Configure EDRs

To enable EDR types for reports:

1. Make sure that the Services Gatekeeper Administration Server is running.
2. Start the Administration Console by entering the following URL in your web browser:

```
http://hostname:port/console
```

Where *hostname* is the DNS name or IP address of the Services Gatekeeper Administration Server, and *port* is the address of the port on which the Administration Server is listening for requests (8001 by default).

3. When the login page appears, enter the user name and the password you used to start the Administration Server (you may have specified this user name and password during the Services Gatekeeper installation process), or enter a user name that has been granted one of the default global security roles.
4. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
5. In the Platform Test Environment or another MBean browser, select: **com.bea.wlcp.wlng.edr.management.EdrServiceMBean**
6. Select the **setEdrTypes** operation.
7. Set these EDR types to true:
   - **Publish_facade_edr**
   - **Publish_enabler_ecr**
   - **Publish_protocolStack_edr**
8. Save your changes.

Deploying the Reports EAR File

To deploy the reports EAR file:

1. Make sure that the Services Gatekeeper Administration Server is running.
2. Start the Administration Console by entering the following URL in your web browser:

   ```
   http://hostname:port/console
   ```

   Where *hostname* is the DNS name or IP address of the Services Gatekeeper Administration Server, and *port* is the address of the port on which the Administration Server is listening for requests (8001 by default).
3. When the login page appears, enter the user name and the password you used to start the Administration Server (you may have specified this user name and password during the Services Gatekeeper installation process), or enter a user name that has been granted one of the default global security roles.
4. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
5. In the left pane of the console, select **Deployments**.
6. In the right pane, click **Install**.
7. On the Locate deployment to install and prepare for deployment page, enter the following path in the **Current Location** field and press Enter.

   ```
   Services_Gatekeeper_home/applications
   ```

8. Select one of the following EDR files and click **Next**:
   - For standalone, single server environments, select **edr_to_analytic-single.ear**.
   - For cluster environments, select **edr_to_analytic.ear**.

9. On the Choose targeting style page, select **Install this deployment as an application**, and click **Next**.
10. On the Select deployment targets page, select the Network Tier servers or clusters that comprise your Services Gatekeeper installation, and click **Next**.
11. On the Optional Settings page, accept the defaults, and click **Next**.
12. Click **Next**.
13. Click **Finish**.
14. In the Change Center click **Activate Changes**.
15. Select your Services Gatekeeper domain and choose **Deployments**.
16. In the **Deployments** table, select **edr_to_analytic** and then click **Start** and choose **Servicing all requests**.
17. On the Start Deployments page, click **Yes**.
18. For clustered environments, ensure that the deployed application is started on all of the Network Tier instances in your installation.

Connecting Services Gatekeeper to the Reports Data Source

To connect Services Gatekeeper to the reports data source:

1. Make sure that the Services Gatekeeper Administration Server is running.
2. Start the Administration Console by entering the following URL in your web browser:

   `http://`*`hostname`*`:`*`port`*`/console`

   Where *hostname* is the DNS name or IP address of the Services Gatekeeper Administration Server and *port* is the address of the port on which the Administration Server is listening for requests (8001 by default).
3. When the login page appears, enter the user name and the password you used to start the Administration Server (you may have specified this user name and password during the Services Gatekeeper installation process), or enter a user name that has been granted one of the default global security roles.
4. In the **Domain Structure** tree, expand **OCSG** and select the Network Tier node with **EdrToAnalytic** deployed.
5. On the **Oracle Communications Services Gatekeeper** page, expand **Container Services** and select **EdrToAnalytic**.
6. In the lower panel, select the **Operations** tab and then choose **connectToDatasource** from the **Select An Operation** list box.
7. Click **Invoke**.
8. Ensure that the operation returns a successful connection.

Verifying the Services Gatekeeper Installation

You should now verify your Services Gatekeeper installation. You can do this by using the Services Gatekeeper Platform Test Environment to send messages through Services Gatekeeper and verify that components are communicating and processing traffic.

Where to Go from Here

If you want to install the Services Gatekeeper Application Test Environment (ATE), go to "Installing the Application Test Environment". Otherwise, see "Next Steps".

7

Configuring the Services Gatekeeper Domain

This chapter describes how to configure an Oracle Communications Services Gatekeeper domain.

Before you configure your domain, you must have set the WebLogic Server home path. See "Services Gatekeeper Post-Installation Tasks".

About Configuring Service Gatekeeper Domains

You must configure the domains of all of your servers before you start them. You can use the WebLogic Server Configuration Wizard to manually configure each server in your installation, or you can configure the domain on your Administration Server and then use the **pack** and **unpack** commands provided by Oracle WebLogic Server to package the configuration data for copying to all the other servers. For more information about packing and unpacking configurations, see *Oracle Fusion Middleware Creating Templates and Domains Using the Pack and Unpack Commands*.

After configuring your Services Gatekeeper domains, return to the "Services Gatekeeper Post-Installation Tasks" for instructions on how to start the Services Gatekeeper servers.

The Services Gatekeeper installer copies the **pack** and **unpack** commands to the *Middleware_home*/**wlserver/common/bin** directory.

About the Domain Configuration Tools

You configure your Services Gatekeeper domain with the following tools:

- The WebLogic Server Configuration Wizard, which can be run in GUI mode or console mode.

  If you want to run the Configuration Wizard in GUI mode on Solaris or Linux, the console attached to the machine on which you are configuring the domain must support a Java-based GUI.

- WebLogic Scripting Tool (WLST), which is a command-line tool that provides configuration scripts.

  System administrators and operators use WLST to monitor and manage WebLogic Server instances and domains. The WLST scripting environment is based on the Java scripting interpreter, Jython. For more information about WLST, see *Oracle Fusion Middleware Understanding the WebLogic Scripting Tool*.

Information Requirements

The Configuration Wizard prompts you for the following information about your database:

- The database hostname
- The database instance name
- The database listener port number
- The names of your managed servers
- The database administrative user name and password

Supporting Dual-Stack IPv4/IPv6 Traffic

You can create communication services that support both IPv4 and IPv6 addresses by creating multiple plug-in instances of that communication service. Create two plug-in instances, one configured for the IPv4 protocol and the other for the IPv6 protocol. For IPv6 support, enter a system's host name instead of an IPv6 address when configuring an MBean. For IPv4 traffic, you can enter the IPv4 address.

Configuring the Domain Using the Configuration Wizard in GUI Mode

The procedure for configuring the domain with the Configuration Wizard follows these steps:

1. If you are running Services Gatekeeper on an IPv6 network, map host names to IPv6 addresses.
2. Start the Configuration Wizard in GUI mode.
3. Answer the questions in each screen of the Configuration Wizard.

For more information about creating a WebLogic domain by using the Configuration Wizard, see "Creating a WebLogic Domain" in *Oracle Fusion Middleware Creating WebLogic Domains Using the Configuration Wizard*.

Mapping Host Names to IPv6 Addresses

If you are running Services Gatekeeper on an IPv6 network, you must first map host names to your IPv6 addresses before running the Configuration Wizard because the wizard cannot accept IPv6 addresses in GUI mode.

To map IPv6 addresses to host names, do the following:

1. In a text editor, open the file **/etc/hosts** (Linux or Solaris) or **\Windows\System32\drivers\etc\hosts** (Windows).
2. Add your IPv6 address-to-host-name mappings to the file in the format:

   ```
   <IPv6 Address>     <host name>     ## Optional comment
   ```

   Your mappings should look similar to the following example:

   ```
   2001:db8:0:f101::1     host-admin.example.com    ## Admin Server
   2001:db8:0:f101::1     host-at1.example.com      ## Application Tier 1
   2001:db8:0:f101::2     host-at2.example.com      ## Application Tier 2
   2001:db8:0:f101::1     host-nt1.example.com      ## Network Tier 1
   2001:db8:0:f101::2     host-nt2.example.com      ## Network Tier 2
   ```

3. Save the file.
4. Flush the local DNS cache for the settings to take effect.

When configuring the domain, you specify the host names in place of the IPv6 addresses.

Starting the Configuration Wizard in GUI Mode

To start the Configuration Wizard in GUI mode:

1. Log in to the target system.
2. Go to the *Middleware_home*/**wlserver/common/bin** directory.
3. At a command prompt, enter one of the following:
   - **Windows**:

     ```
     config
     ```

   - **Linux or Solaris**:

     ```
     sh config.sh
     ```

The Configuration Wizard starts and the Configuration Type screen appears. Go to "Configuring the Domain in GUI Mode" and follow the steps for configuring the domain.

Configuring the Domain in GUI Mode

The procedure in this section reflects using the Configuration Wizard in GUI mode, but the screen names are the same in GUI mode and console mode.

Important:

- Configure only one domain at a time.
- Each domain must be created in its own, empty directory.
- If you will be using CORBA-based functionality that connects to multiple hosts, do not use the value **localhost** in any configurations. Use an actual IP address or fully qualified host name instead.

The Configuration Wizard displays a sequence of screens, in the order listed below. The screens that you will see depend on the type of product configuration template that you select in the Templates screen. To configure your domain, answer the questions in the following screens:

- Configuration Type Screen
- Templates Screen
- Administrator Account Screen
- Domain Mode and JDK Screen
- JDBC Data Sources Screen
- JDBC Data Sources Test Screen
- Advanced Configuration Screen

- Configuration Summary Screen
- Configuration Progress Screen
- Configuration Success Screen

Configuration Type Screen

In the Configuration Type screen:

1. Select **Create a new domain**.
2. In the **Domain Location** field, enter the target domain directory or use the **Browse** button to locate the directory.

   The directory you enter must be empty.
3. Click **Next**.

Templates Screen

In the Template screen:

1. Select **Create Domain Using Product Templates**.
2. In the **Available Templates** area, select only *one* of the following Services Gatekeeper configuration templates.
   - Basic Oracle Communications Services Gatekeeper Domain
   - OCSG Basic HA Configuration
   - OCSG Domain with Access and Network Clusters
   - OCSG Domain with Access and Network Clusters with Oracle RAC Configuration
   - OCSG Portal Domain

   Note: You can configure only one Services Gatekeeper template at a time.
3. Click **Next**.

Administrator Account Screen

In the Administrator Account screen:

1. Enter the main administrator user name.

   This name is used to start the Administration Server and connect to it. The default user name is **weblogic**, which you can use for domain setup and testing. User names are case sensitive. Do not use commas or any characters in the following comma-separated list:

   ```
   \t, < >, #, |, &, ?, ( ), { }
   ```
2. Enter the main administrator password.

   The password is case sensitive and must contain a minimum of eight characters, at least one of which is not alphabetic.
3. Click **Next**.

Domain Mode and JDK Screen

In the Domain Mode and JDK screen:

1. In the **Domain Mode** area, select the appropriate startup mode for your installation:
   - Development Mode
   - Production Mode (This is the only supported mode for 64-bit Solaris environments.)

   If you select **Production Mode**, do not enable SSL unless you have a trusted key. For more information about startup modes, see "Tuning WebLogic Server" in *Fusion Middleware Performance and Tuning for Oracle WebLogic Server*.
2. In the **JDK** area, select the JDK to use for the domain.

   By default, the installer selects the JDK that was used when you installed Services Gatekeeper. Alternatively, you can specify a different JDK.
3. Click **Next**.

JDBC Data Sources Screen

Specify the connection information between Services Gatekeeper and the JDBC data sources (databases).

In the JDBC Data Sources screen:

1. In the table, select the **wlng.datasource** and **wlng.localTX.datasources** checkboxes to configure these data sources simultaneously. To configure these data sources separately, make adjustments in the data source for the transactional data source.
2. Typically, fields you may need to edit include:
   - **Vendor**: The database vendor. The default is **Oracle**. Select **MySQL** if you are using a MySQL database or cluster.
   - **Driver**: The driver for your database type. The available drivers are specific to the vendor value you specified.

     For Oracle databases, the default is Oracle's Driver (Thin) for Instance connections. For non-Oracle RAC domains, use the **non-XA** thin driver for **wlng.localTX.datasource**, and the **XA** driver for **wlng.datasource**.

     For MySQL databases and clusters, select the **com.mysql.jdbc.Driver** for all data sources.
   - **DBMS/Service**: The name of the database you created in "Installing the Database". The default is **SLEE_DB**.
   - **Host Name:** The location of the database. The default is **localhost**.
   - **Port**: The port number for contacting the database. For Oracle, the default is **1521**. For MySQL, the default is **3306**.
   - **Username**: The Services Gatekeeper user name you created when you installed the database. The default is **SETME_DBUSER**.
   - **Password**: The Services Gatekeeper password you created when you installed the database.
   - **Oracle RAC configuration for data sources**: If you are using Real Application Cluster features, do one of the following:

  - To convert one or more data sources to GridLink Oracle RAC data sources, select **Convert to GridLink**.
  - To convert one or more data sources to Oracle RAC multi-data sources, select **Convert to RAC multi data source**.
  - To not convert the data sources, select **Don't Convert**.

3. Click **Next**.

JDBC Data Sources Test Screen

The JDBC Data Sources Test screen automatically tests your data source configurations:

- A green check mark displayed in the **Status** column indicates that the configuration is valid.
- A red circle indicates a problem.

  The bottom of the screen shows a short error message to help you troubleshoot the problem. Fix the error and click **Test Selected Connections** to test your data source configurations again.

Click **Next** when you are ready to proceed to the next screen.

Advanced Configuration Screen

The Advanced Configuration screen allows you to perform advanced configuration on the listed items. If you are happy with the current settings, keep all of the checkboxes deselected and click **Next**.

1. In the Advanced Configuration screen, select one or more of the following checkboxes and then click **Next**.
   - Administration Server
   - Node Manager
   - Managed Servers, Clusters and Coherence
   - Deployments and Services

   The next screen that appears depends on the checkboxes that you selected.
2. If you selected **Administration Server**, the Administration Server screen appears.

   Add or change the Administration Server name, listen address, and listen port. Do not enable SSL unless you have a trusted key. Click **Next**.
3. If you selected **Node Manager**, the Node Manager screen appears.

   Select the node manager type, enter the node manager credentials, and then click **Next**.
4. If you selected **Manager Servers, Clusters and Coherence**, do the following:
   a. In the Managed Servers screen, add or change the connection information for the managed servers. Each managed server is an instance of Oracle WebLogic Server.

      Click **Add** for each manager server that you want to create. Enter the server name, listen address, and listen port. Do not enable SSL unless you have a trusted key. Click **Next**.
   b. In the Clusters screen, click **Add** for each cluster that you want to create. For example **203.0.113.164:8001, 203.0.113.165:8001**.

Enter the information about your cluster and frontend. Click **Next**.

c. In the Coherence Clusters screen, accept the default cluster name and port number or type new ones. Click **Next**.

d. In the Machines screen, add or change information about each machine.

In the context of WebLogic Server, a machine is the logical representation of the system that hosts one or more WebLogic Server instances, for the purposes of starting and stopping remote servers using the node manager. In a domain, machine definitions identify a particular, physical piece of hardware and are used to associate a computer with the managed servers it hosts.

5. If you selected **Deployments and Services**, do the following:

a. In the Deployments Targeting screen, target one or more applications to a server or cluster. Select one or more applications in the **Deployments** pane, select one server or cluster in the **Targets** pane, and then click the right arrow button.

b. In the Services Targeting screen, target services to servers or clusters. Select one or more services in the **Services** page, select a server or cluster in the **Targets** pane, and then click the right arrow button.

c. Click **Next**.

Configuration Summary Screen

The Configuration Summary screen displays the previously configured domain settings. Use the **View** drop-down list to choose a category view.

Click **Create** to accept the domain details and start creating the domain.

Configuration Progress Screen

The Configuration Progress screen displays a progress bar that indicates the status of the configuration process. When the configuration progress is complete, click **Next**.

Configuration Success Screen

The Configuration Success screen displays the domain's location and Administration Server URL for accessing the domain.

Click **Finish** to end your configuration session.

Configuring the Domain Using the Configuration Wizard in Console Mode

This section describes how to configure the domain by using the Configuration Wizard in console mode.

Starting the Configuration Wizard in Console Mode

To start the Configuration Wizard in console mode:

1. Log in to the target system.
2. Open a command window.
3. Go to *Middleware_home***/wlserver/common/bin**.
4. At the prompt, enter one of the following commands and press Enter:
   - Windows:

```
config -mode=console
```

- Linux and Solaris:

```
sh config.sh -mode=console
```

The Configuration Wizard starts in console mode and the Welcome screen appears.

Configuring the Domain in Console Mode

To configure your domain, respond to the prompts in each section by entering the number associated with your choice and pressing **Enter**, or by typing **`Next`** or **`n`** to accept the current selection.

The right arrow (->) indicates the value currently selected. To quit the Configuration Wizard, type **`Exit`** or **`x`** in response to any prompt. To review or change your selection, type **`Previous`** or **`p`** at the prompt.

The screen names and parameters in the Configuration Wizard are the same for both GUI and console modes. See "Configuring the Domain in GUI Mode" for instructions on setting the configuration parameters.

Note: After creating a new domain in console mode, you must copy the *domain_home*/**security/SerializedSystemIni.dat** file from the administration server to the same location on the new domain.

Configuring the Domain Using a WebLogic Scripting Tool Script

This section explains how to configure a Services Gatekeeper domain by using a WebLogic Scripting Tool (WLST) script.

The WLST scripting environment is based on the Java scripting interpreter, Jython. For more information about WLST, see "Using the WebLogic Scripting Tool" in *Oracle Fusion Middleware Understanding the WebLogic Scripting Tool*.

Caution: WLST has a significant learning curve. If you do not know how to use WLST and do not wish to spend the time to become familiar with it, use the Configuration Wizard to set up your domains instead.

Setting Up Your Environment

You must set environment variables for WLST to run properly.

1. Log in to the target system.
2. Open a command window.
3. Go to *Middleware_home*/**wlserver/server/bin**.
4. At the prompt, enter one of the following commands:
   - **Windows**:

     ```
     setWLSEnv.cmd
     ```

   - **Linux and Solaris**:

```
sh setWLSEnv.sh
```

Choosing the WLST Domain Setup Script

Services Gatekeeper provides five WLST domain setup scripts and five corresponding domain configuration templates. The scripts are located in *Middleware_home*/**wlserver/common/templates/scripts/wlst**, and the templates are located in *Middleware_home*/**wlserver/common/templates/wls**.

Table 7–1 describes the scripts and their respective domain templates used to configure each type of domain:

Table 7–1 Scripts and Domain Templates

Script	Template	Description
basic-ocsg-ha.py	basic-ocsg-ha-domain.jar	Creates a basic domain with two servers, each with an Access Tier, a Network Tier instance, and a database. Database replication must be set up separately.
ocsg-database-setup.py	ocsg-domain.jar	Creates a basic all-in-one domain typical of development environments.
access-network-cluster.py	ocsg-access-network-domain.jar	Creates a domain with separate access and network clusters.
ocsg-osb-integ.py	ocsg-osb-integ-domain.jar	Creates a domain with separate access and network clusters with the additional data sources that an Oracle RAC installation requires.

Configuring the WLST Script

You must configure the WLST domain setup script to work with your environment. This section describes the configurations you may need to perform.

Configuring Multicluster Settings

Perform this task if you are using a domain setup script other than **wlng-cluster.py**.

If you are setting up the standard version of one of the multi-cluster domains, only a few variables need to be set at the beginning of the script. This procedure describes how to modify the WLST script to set the multicluster settings in the section called **Configuration (INPUT) Parameters**. Example 7–1 shows the necessary configuration parameters that need to be edited for your environment.

Example 7–1 Configuration (INPUT) Parameters Section from Access-Network-rac.py

```
#===============================================================================
# Configuration (INPUT) Parameters
#===============================================================================

# listen address input parameters
# example: hostname can be DNSName or IPAddress

AdminServerListenAddress = "host-admin.bea.com"
AdminServerListenPort    =  7001
NT1ServerListenAddress   = "host-nt1.bea.com"
NT1ListenPort            =  8001
NT2ServerListenAddress   = "host-nt2.bea.com"
NT2ListenPort            =  8001
AT1ServerListenAddress   = "host-at1.bea.com"
AT1ListenPort            =  8001
```

```
AT2ServerListenAddress   = "host-at2.bea.com"
AT2ListenPort            =  8001

NTClusterAddress         = "host-nt1.bea.com:8001,host-nt2.bea.com:8001"
ATClusterAddress         = "host-at1.bea.com:8001,host-at2.bea.com:8001"

NTClusterMultiCastAddress = '237.0.0.101'
NTClusterMultiCastPort    = 8050
ATClusterMultiCastAddress = '237.0.0.102'
ATClusterMultiCastPort    = 8050

# DataSource Settings

# RAC Node-1 Settings

RACNode1URL      = "SETME_URL"

# RAC Node-2 Settings

RACNode2URL      = "SETME_URL"

# Database settings

OracleXADriver    = "SETME_XADRIVER"
OracleNonXADriver = "SETME_nonXADRIVER"
DBUser            = "SETME_USER"
DBPassword        = "SETME_PASSWORD"
```

To configure the multicluster settings:

1. Set the listen address and listen port for the Administration Server, the two Access Tier servers, and the two Network Tier servers.
   - Replace the **host*.bea.com** values with either the DNS name or the IP Address of the appropriate servers.
   - Replace the listen port values as necessary. The listen address and port combinations must be unique.
2. Fill in the appropriate listen address and port combinations to assign the servers to the appropriate clusters. The entry should be comma delimited, with no spaces.
3. Fill in the appropriate multicast addresses values for each cluster.
4. If using a configuration script for Oracle RAC deployments:
   - Set the appropriate URLs for each of the Oracle RAC instances.
   - Set the appropriate values for the transactional (XA) and localTX(nonXA) datasources.
5. For non-Oracle RAC deployments:
   - Set the appropriate values for the **wlng.datasource**.
   - Set the appropriate values for the **wlng.localTX.datasource**. The values should be non-XA.
6. (Optional) To use the Administration Console and node manager to start remote servers, change the **NodeManager ListenAddress** values in the **Configure Managed Servers** section by editing the following line for each managed server:

   ```
   set('ListenAddress','localhost')
   ```

7. (Optional) Change the **localhost** value to the correct listen address for your environment.

   The default domain user (weblogic) and password.

Adding Machines and Servers to a Multicluster Configuration

Perform this task if you are using either the **access-network-cluster.py** or the **access-network-rac-cluster.py** domain setup script for cluster configuration and you also want to create additional machines, servers, or both.

> **Note:** You can also add servers and machines using the Administrative Console after you set up your primary Services Gatekeeper domain, which is a simpler way of adding machines and servers.

Using WLST in offline mode, which is the mode that Services Gatekeeper scripts use, allows accessing and updating only those configuration objects that have been previously persisted to a configuration file. All the provided WLST scripts create this configuration file automatically as they run, but each script adds only those objects that are specified in the domain templates they support. If you must add more configuration objects, such as additional managed servers or machines, you must add additional parameters to the script to create them before you can configure them. The specific parameters you add depend on how your installation is set up.

Adding Machines

Use the sample code in Table 7–2 to add machines in the script *before* you assign managed servers to them.

Table 7–2 Code to Add Machines

Comment Section	Code to add	Value

Configure managed servers	`cd('/')`
	`create('new_Machine_5','Machine')`
	`cd('Machine/new_Machine_5')`
	`create('new_Machine_5','NodeManager')`
		Add as many of these statements as you need, replacing *new_Machine_5* with your machine name.

Adding Managed Servers

After you add machines, you can assign managed servers to them. You can also add new managed servers. In the sample code in Table 7–3, a new managed server is created and then assigned to *new_Machine_5*, created in the previous section.

Table 7–3 Code to Create Additional Managed Servers

Comment Section	Statement to edit	Value

Configure managed servers	`cd('/')`
	`create('new_Server_1', 'Server')`
	`cd('Server/new_Server_1')`
	`set('ListenPort', 'port')`
	`set('ListenAddress', address)`
	`set('Machine','new_Machine_5')`
		Create new servers as needed, and set the **ListenAddress**.
		The *new_Server_1* is the name of the new server being created, *port* is the listen port for the server, *address* is the IP address or DNS name of the new server and *new_Machine_5* is the machine to which you are adding the new server.

Setting the NodeManager Listen Address

You must also add a section to configure the **Listen Address** of any new machine (and its node manager) you are adding. The sample code in Table 7–4 shows the WLST statement used to complete this configuration.

Table 7–4 Setting Listen Address for Node Manager

Comment Section	Statement to add	Value

Configure managed servers	`cd('/')`
	`cd('Machine/new_Machine_5')`
	`set('Name','new_Machine_5')`
	`set('Address','address')`
	`cd('NodeManager/new_Machine_5')`
	`set('ListenAddress','new_Server_1')`
	`set('ListenPort','port')`
		One section per added machine is required.
		The *new_Server_1* is the name of the new server being created, *port* is the listen port for the server, *address* is the IP address or DNS name of the new server and *new_Machine_5* is the machine to which you are adding the new server.

Assigning New Managed Servers to a Cluster

You must assign any newly-created managed servers to their appropriate cluster by adding an **assign** command. The sample code in Table 7–5 shows a WLST statement that assigns new managed servers to a cluster.

Table 7–5 Assigning New Managed Servers

Comment Section	Statement to add	Value

Configure a cluster and assign the Managed Servers to that cluster.	`cd('/')`
	`[standard]`
	`assign('Server', 'new_Server_1','Cluster','cluster1')`
		One line per added Managed Server is required.
		The *new_Server_1* is the name of the new server you created and *cluster1* is the cluster you are adding the server to.

Preventing Communication Services from Being Deployed

Perform this task if you know that you will not use one or more communication services and you prefer to prevent them from being deployed.

> **Note:** You can also undeploy communication services at a later time. See *Services Gatekeeper System Administrator's Guide* for information about undeploying communication services.

All communication services consist of two EAR files: an Access Tier file and a Network Tier file. To prevent a communication service from being deployed, add an **unassign** command to your script for both EAR files.

For example, to prevent the PX 3.0 Third Party Call communication service from being deployed, add the following example section to your script:

```
#=====================================================================
# Unassign applications to target
#=====================================================================
cd('/')
unassign('Application', 'wlng_at_third_party_call_px30#4.0 ', 'Target', 'WLNG_AT_
Cluster')
unassign('Application', 'wlng_nt_third_party_call_px30#4.0 ', 'Target', 'WLNG_NT_
Cluster')
```

Running the WLST Domain Setup Script

After editing the WLST domain setup script, run it using the following command:

```
java weblogic.WLST script_name.py
```

Where *script_name* is the name of the WLST script.

Where to Go From Here

Complete the rest of the Services Gatekeeper post installation tasks, picking up at "Creating JMS Servers for Additional Network Tier Servers".

8

Installing Services Gatekeeper Reports

This chapter describes how to set up and install Oracle Communications Services Gatekeeper Reports.

For more information about reports, see "Managing and Configuring Statistics and Transaction Licenses" in *Services Gatekeeper System Administrator's Guide*.

Overview of Installing Services Gatekeeper Reports

The procedure for installing Services Gatekeeper Reports follows these steps:

1. Install Services Gatekeeper. See "Installing Services Gatekeeper".
2. Perform pre-installation tasks for reports:
   - Install Oracle Business Intelligence.
   - Configure Oracle Business Intelligence for use with Services Gatekeeper.
3. Install Services Gatekeeper Reports.
4. Enable Oracle Business Intelligence Write-back and Iframe Support.
5. Perform post-installation tasks, which include configuring the Services Gatekeeper domain and performing post-installation tasks for Reports. See "Post-Installation Tasks for Reports".

After installing and configuring Services Gatekeeper Reports, Services Gatekeeper reports and statistics can be found in your Oracle Business Intelligence dashboard in the **EDR Analysis Home Page**.

Reports System Requirements

Reports is supported on the following:

- WebLogic Server 10.3.5 or higher
- Oracle Business Intelligence 11*g*
- JDK 1.7.0_15 or higher, plus the latest security updates

Installation Prerequisites

Before installing Services Gatekeeper Reports, you must first install and configure Oracle Business Intelligence, which hosts the reporting functionality. You must also install a separate database to serve as the reports staging repository.

Installing Oracle Business Intelligence

The general steps for installing Oracle Business Intelligence are:

1. Ensure that your system environment can host Oracle Business Intelligence.
2. Install a database and populate that database with the required schemas by using the Repository Creation Utility (RCU) tool.
3. Download and run the Oracle Business Intelligence installer.
4. Configure Oracle Business Intelligence.

For comprehensive installation instructions, see *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence 11g Release 1* at the Oracle Help Center web site:

http://docs.oracle.com/cd/E28280_01/bi.1111/e10539/toc.htm

Configuring Oracle Business Intelligence

This section describes the tasks you perform to configure Oracle Business Intelligence.

Setting Configuration Permissions

Set the Oracle Business Intelligence administrator role permissions:

1. Access the Oracle Business Intelligence Presentation Services console using a supported web browser.
2. Select **Administration**.
3. In the Security section, select **Manage Privileges**.
4. Click the **Admin: General** tab.
5. Select the **BI Administrator Role** permissions link for **See privileged errors**.
6. Set the permission to **Denied**.
7. Click **OK**.
8. Select the **BI Administrator Role** permissions link for **See SQL issued errors**.
9. Set the permission to **Denied**.
10. Click **OK**.

Creating the Reports Repository Database and User

After you have installed and configured Oracle Business Intelligence, you must create a database user that has access to the reports staging data. Depending on your requirements, you can use the same database that supports Oracle Business Intelligence or you can use a separate database instance. Ensure that the database user has the following permissions:

- connect
- resource
- create any table
- create job

Refer to your database documentation for information about creating database users and granting permissions.

Configuring the Services Gatekeeper RPD File

You must configure an Oracle Business Intelligence repository (RPD) file for Oracle Business Intelligence by using the Oracle Business Intelligence Administration Tool. The file contains the data storage schema for Services Gatekeeper.

The Services Gatekeeper installer creates an RPD file (**edr.rpd**) for Services Gatekeeper in *Middleware_home***/ocsg/ext/analytics**. The file's default password is **Orcl123456**. For security, use the Oracle Business Intelligence Administration Tool to change the password.

To configure the Services Gatekeeper RPD file:

1. Open the *Middleware_home***/ocsg/ext/analytics/edr.rpd** file in the Oracle Business Intelligence Administration Tool.
2. Change the default password.
3. Edit the **orcl** and **blockInit** database connection information to reference your database.
4. Transfer the **edr.rpd** file to the machine hosting your Oracle Business Intelligence installation.

For instructions about configuring RPD files, including changing the password and setting database connection information, see "Importing Metadata and Working with Data Sources" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

Gathering Required Oracle Business Intelligence System Information

Gather the following information from your Oracle Business Intelligence installation, which you will need when you install Services Gatekeeper Reports:

- The Oracle Business Intelligence Administration Console URL
- The Oracle Business Intelligence Administration Console login name and password
- The reports database host name and port number
- The reports DBMS/Service
- The reports database user name and password
- The file path to the configured Services Gatekeeper RPD file
- The password for the Services Gatekeeper RPD file
- The Oracle Business Intelligence *Oracle_instance* path from your Oracle Business Intelligence installation

Installing Services Gatekeeper Reports

The Reports installer runs in GUI mode only. You can create an installation log by using the **-log=***logfilename* parameter on the command line when you run the installer. For more information about creating a log file, see "Creating an Installation Log".

Caution:

- Before continuing, make sure that all components of your Oracle Business Intelligence installation are running, including administration servers, database servers, and any associated domains.
- Services Gatekeeper Reports requires administrator access if you are installing it on a Windows-based host system.

To install Reports, do the following on the system that is hosting Oracle Business Intelligence:

1. If you are installing on a 64-bit system, ensure that a 64-bit JDK or a hybrid 32/64-bit JDK is installed on the target machine.

   If it is not installed, install one. See "Services Gatekeeper System Requirements" for information about supported JDK versions.

2. Run the `java -version` command, or `java -d64 -version` command on platforms using a 32/64-bit hybrid JDK, to ensure that the JAVA_HOME environment variable is set to a 64-bit JDK.

   If JAVA_HOME is not correctly set, set it to point to the correct JDK.

3. Add the **bin** directory of the appropriate JDK to the beginning of the PATH variable definition. For example:

   ```
   PATH=$JAVA_HOME/bin:$PATH
   export PATH
   ```

4. Download the Services Gatekeeper Reports installer from the Oracle software delivery website:

   `https://edelivery.oracle.com/`

5. Change to the directory where you downloaded the installation program.

6. To start the installer, do one of the following:

   - To start the installer on a system that uses a 32/64-bit hybrid JDK, enter:

     ```
     java -d64 -jar ocsg_analytics_generic.jar [-log=logfilename]
     ```

   - To start the installer on a 32-bit system, enter:

     ```
     java -jar ocsg_analytics_generic.jar [-log=logfilename]
     ```

   After the installer starts, the Welcome screen appears.

7. Click **Next**.

   The Installation Location screen appears.

8. In the **Oracle Home** field, enter the full path to your Middleware home directory or use the **Browse** button to locate the directory.

   The Middleware home directory is the central directory for all Oracle products installed on the target system, such as WebLogic Server, Services Gatekeeper, and Services Gatekeeper Reports.

   To see a list of Oracle products that are currently installed in the directory, click **View**.

9. Click **Next**.

   The Installation Type screen appears.

10. Click **Next**.

    The Analytics Parameters screen appears.

11. In the **OBIEE Admin Console** area, enter the following information:

    - **URL**: The URL of the OBIEE Administration Console. For example, **http://server.com:8001/console**.
    - **User Name**: The Oracle Business Intelligence WebLogic domain administrator user name.
    - **Password**: The password for the Oracle Business Intelligence WebLogic domain administrator.

12. In the **Oracle Database for Analytics** area, enter the following information:

    - **Host Name**: The host name of the database server to be used for reports data.
    - **Port**: The port number through which the database host listens.
    - **DBMS/Service**: The name of the database or service hosting the reports data.
    - **User Name**: The user name that will access the reports database.
    - **Password**: The password for the database user.

13. In the **OBIEE stuff for Analytics** area, enter the following information:

    - **RPD file Path**: The local path to the updated Services Gatekeeper RPD file including the name of the RPD file. For example, **/export/home/oracle/edr.rpd**.
    - **RPD file Password**: The password used to access the reports repository.
    - **OBIEE ORACLE_INSTANCE path**: The Oracle instance location, defined when Oracle Business Intelligence was installed. For example, *Middleware_home*/**instances/instance1**.

14. Click **Next**.

    The Prerequisite Checks screen appears.

15. The screen automatically tests your system to ensure that it meets all operating system and JDK software requirements:

    - A green check mark indicates that your system passed the prerequisite check.
    - A red circle indicates a problem. The bottom of the screen shows a short error message to help you troubleshoot the problem. Fix the error and click **Rerun** to perform the prerequisite checks again. To continue the installation without fixing the problem, click **Skip**.

16. Click **Next**.

    The Installation Summary screen appears.

17. Click **Next**.

    The Installation Summary screen appears.

18. Ensure that the listed installation location and feature sets to install are correct.

    If the list is not correct, you can use the **Back** button to make corrections.

    To save the information to a response file so you can install the component later, click **Save Response File** and specify the name and location of the response file.

19. Click **Install** to start the installation.

    The Installation Progress screen appears, and a progress bar indicates the status of the installation process.

20. Click **Next**.

21. When the Installation Complete screen appears, click **Finish**.

    The installer exits.

22. Check the WebLogic Server Administration Console log for errors.

23. Restart your Oracle Business Intelligence instance for the changes to take effect.

24. Complete the procedures in "Enabling Oracle Business Intelligence Write-Back and Iframe Support".

Enabling Oracle Business Intelligence Write-Back and Iframe Support

You must make the following modifications to your Oracle Business Intelligence installation:

- Enable Oracle Business Intelligence write-back support for parameter/value-related reports.
- Enable Oracle Business Intelligence Iframe support to support portal integration.

> **Note:** Make these configuration changes on every Oracle Business Intelligence server in a clustered environment.

To enable Oracle Business Intelligence write-back and Iframe support:

1. Go to *Middleware_home***/ocsg/ext/analytics**.

2. Copy the write-back template file (**write_back.xml**) to the following location:

   *Oracle_instance***/bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips***n***/analyticsRes/customMessages**

   where *Oracle_instance* is the Oracle Business Intelligence instance path and *n* is replaced by the Oracle Business Intelligence instance number.

3. Open the **instanceconfig.xml** file located at *Oracle_instance***/config/OracleBIPresentationServicesComponent/coreapplication_obips***n*.

4. Locate the `ServerInstance` element and add it to the `LightWriteback` element:

```
<WebConfig>
   <ServerInstance>
      <LightWriteback>true</LightWriteback>
   </ServerInstance>
<WebConfig>
```

5. Locate the `Security` element and add to it the `InIFrameRenderingMode` element:

```
<Security>
   <InIFrameRenderingMode>allow</InIFrameRenderingMode>
   <!--This Configuration setting...-->
   <ClientSessionExpireMinutes>210</ClientSessionExpireMinutes>
</Security>
```

6. Save your changes and close the file.
7. Restart Oracle Business Intelligence.
8. Access the Oracle Business Intelligence Presentation Services console using a supported browser. The default address is http://*OBI_host*:9704, where *OBI_host* is the Oracle Business Intelligence host.
9. In the Oracle Business Intelligence Presentation Services console, go to **Settings**, then **Administration**, and then **Manage Privileges**.
10. Grant the privilege **Write Back to database** to the appropriate group.

Configure OBIEE Caching For Improved Performance

Services Gatekeeper uses Oracle Business Intelligence Enterprise Edition (OBIEE) for reporting. The OBIEE default behavior is to cache data in the BI server and presentation server caches before making it available to use. You can also use OBIEE data dynamically if your implementation requires it. However, the price is system performance. Dynamic data requires a significantly more bandwidth than cached data.

To turn these OBIEE caches off and use the data dynamically:

- Disable the presentation server caching by adding these entries to the *OBIEE_home*/**instances/instance1/config/OracleBIPresentationServicesComponent/coreapplication_obips1/instanceconfig.xml** file:

```
<Cache>
.
    <Query>
.
      <MaxEntries>1</MaxEntries>
.
      <MaxExpireMinutes>-1</MaxExpireMinutes>
.
      <MinExpireMinutes>-1</MinExpireMinutes>
.
      <MinUserExpireMinutes>-1</MinUserExpireMinutes>
.
    </Query>
.
  </Cache>
```

- Disable the BI server cache. You can find example instructions at the OBIEE training web site:

  http://obieetraining11.blogspot.com/2012/08/obiee-11g-disable-caching.html

See the OBIEE documentation for information on these caches.

Where to Go from Here

Perform the remaining post-installation tasks for Reports in "Post-Installation Tasks for Reports".

9

Installing the Platform Test Environment

This chapter describes how to install Oracle Communications Services Gatekeeper Platform Test Environment (PTE).

PTE is a graphical user interface (GUI) tool that you use to test default Services Gatekeeper features and your own custom communication services. For more information about PTE, see "Understanding the Platform Test Environment" in *Services Gatekeeper Platform Test Environment User's Guide*.

Overview of Installing PTE

You download and install the PTE separately from other Services Gatekeeper software.

The procedure for installing Services Gatekeeper PTE follows these steps:

1. Install Services Gatekeeper. See "Installing Services Gatekeeper".
2. Install Services Gatekeeper PTE.
3. Perform post-installation tasks, such as connecting PTE to Services Gatekeeper and configuring your communication services. See "Configuring and Maintaining Your PTE Server Environment" in *Services Gatekeeper Platform Test Environment User's Guide*.

After installing and configuring Services Gatekeeper PTE, you can start it in GUI mode or console mode. For more information, see "Starting the PTE" in *Services Gatekeeper Platform Test Environment User's Guide*.

Installing the PTE in GUI Mode

You can create an installation log by using the **-log=***logfilename* parameter on the command line when you run the installer. For more information about creating a log file, see "Creating an Installation Log".

> **Note:** Services Gatekeeper PTE requires administrator access if you are installing it on a Windows-based host system.

To install PTE:

1. Log in to the target system.
2. Download the Services Gatekeeper PTE installer from the Oracle software delivery website:

   `https://edelivery.oracle.com/`

3. Change to the directory where you downloaded the software.
4. Start the installer:

   ```
   java -jar ocsg_pte_generic.jar [-log=logfilename]
   ```

   After the installer starts, the Welcome screen appears.
5. Click **Next**.

   The Installation Location screen appears.
6. In the **Oracle Home** field, enter the full path to your Middleware home directory or use the **Browse** button to locate the directory.

   The Middleware home directory is the central directory for all Oracle products installed on the target system, such as WebLogic Server, Services Gatekeeper, and Services Gatekeeper PTE.

   To see a list of Oracle products that are currently installed in the directory, click **View**.
7. Click **Next**.

   The Installation Type screen appears.
8. Click **Next**.

   The Prerequisite Checks screen appears.
9. The screen automatically tests your system to ensure that it meets all operating system and JDK software requirements:
   - A green check mark indicates that your system passed the prerequisite check.
   - A red circle indicates a problem. The bottom of the screen shows a short error message to help you troubleshoot the problem. Fix the error and click **Rerun** to perform the prerequisite checks again. To continue the installation without fixing the problem, click **Skip**.
10. Click **Next**.

    The Installation Summary screen appears.
11. Ensure that the listed installation location and feature sets to install are correct.

    If the list is not correct, you can use the **Back** button to make corrections.

    To save the information to a response file so you can install the component later, click **Save Response File** and specify the name and location of the response file.
12. Click **Install** to start the installation.

    The Installation Progress screen appears, and a progress bar indicates the status of the installation process.
13. Click **Next**.
14. When the Installation Complete screen appears, click **Finish**.

Installing the PTE in Silent Mode

This section describes how to install the PTE in silent mode on all platforms.

Use silent mode for installing duplicate installations on multiple machines. You do this by creating and using the **response.rsp** configuration file, and then specifying it as a

parameter during a silent mode installation. When silent mode is used, the installation program does not display any options during the installation process.

To install the PTE in silent mode:

1. Log in to the target system.
2. Download the Services Gatekeeper PTE installer from the Oracle software delivery website:

   https://edelivery.oracle.com/

3. Create a **response.rsp** file in a text editor.
4. Add the following contents to the file:

```
[ENGINE]

#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

#The oracle home location. This can be an existing Oracle Home or a new Oracle
Home
ORACLE_HOME=Middleware_home

#Set this variable value to the Installation Type selected. For example, .
INSTALL_TYPE=PTE
```

5. Save the file in the directory where you downloaded the PTE package.
6. From the directory where you downloaded the PTE package, enter:

```
java -jar ocsg_pte_generic.jar -silent -responseFile ResponseFile
```

   where *ResponseFile* is the full path and name of the Response File. For example, **/home/use/bin/response.rsp**.

The installation proceeds with no prompts.

Where to Go from Here

To finish setting up PTE, perform the post installation tasks described in "Configuring and Maintaining Your PTE Server Environment" in *Services Gatekeeper Platform Test Environment User's Guide*.

If you want to install Services Gatekeeper Application Test Environment (ATE), see "Installing the Application Test Environment". Otherwise, perform the tasks described in "Services Gatekeeper Post-Installation Tasks".

10

Installing the Application Test Environment

This chapter explains how to install the Oracle Communications Services Gatekeeper Application Test Environment (ATE), which is a graphical user interface tool for testing Services Gatekeeper applications.

For more information about ATE, see "Understanding the Application Test Environment" in *Services Gatekeeper Application Developer's Guide*.

Overview of Installing Services Gatekeeper Application Test Environment

You download and install the ATE separately from other Services Gatekeeper software. You do not need to install Services Gatekeeper to install and run the ATE.

The procedure for installing Services Gatekeeper ATE follows these steps:

1. Set your environment variables to point to the JRE.
2. Install Services Gatekeeper ATE.

For information on how to use the features in ATE, see "Testing Applications with the Application Test Environment" in *Services Gatekeeper Application Developer's Guide*.

ATE System Requirements

The ATE is supported on the following operating systems:

- Windows 7
- Redhat Linux, Version 6
- Mac OS X 10.6

The ATE requires JDK 1.7.0_15 or higher, plus the latest security updates.

Setting Your Environment Variables for ATE

Install JRE on your system and set your environment variables.

To set up your system for ATE installation:

1. If a JDK is not already installed on your system, install it. See "ATE System Requirements" for the supported JDK versions.
2. Set the **JAVA_HOME** environment variable to the JRE **bin** directory.
3. Add the JRE **bin** directory to your **PATH** environment variable.

Installing the ATE in GUI Mode

This section describes how to install the ATE in GUI mode.

> **Note:** Services Gatekeeper ATE requires administrator access if you are installing it on a Windows-based host system.

To install the ATE in GUI mode:

1. Download the ATE installer from the Oracle software delivery website:

   https://edelivery.oracle.com/

2. Open a command window on the system where you are installing the ATE.
3. From the directory where you downloaded the ATE package, do one of the following:
   - To start the installer on Windows or Linux, enter:

     ```
     java -jar ocsg_sdk_generic.jar
     ```

   - To start the installer on Mac OS X, enter:

     ```
     java -Dos.name=unix -jar ocsg_sdk_generic.jar
     ```

   After you start the installer, the Welcome screen appears.
4. Click **Next**.

   The Installation Location screen appears.
5. In the **Oracle Home** field, enter the full path to your Middleware home directory or use the **Browse** button to locate the directory.

   The Middleware home directory is the central directory for all Oracle products installed on the target system, such as WebLogic Server, Services Gatekeeper, and Services Gatekeeper ATE.

   To see a list of Oracle products that are currently installed in the directory, click **View**.
6. Click **Next**.

   The Installation Type screen appears.
7. Click **Next**.

   The Prerequisite Checks screen appears.
8. The screen automatically tests your system to ensure that it meets all operating system and JDK software requirements:
   - A green check mark indicates that your system passed the prerequisite check.
   - A red circle indicates a problem. The bottom of the screen shows a short error message to help you troubleshoot the problem. Fix the error and click **Rerun** to perform the prerequisite checks again. To continue the installation without fixing the problem, click **Skip**.
9. Click **Next**.

   The Installation Summary screen appears.
10. Ensure that the listed installation location and feature sets to install are correct.

If the list is not correct, you can use the **Back** button to make corrections.

To save the information to a response file so you can install the component later, click **Save Response File** and specify the name and location of the response file.

11. Click **Install** to start the installation.

    The Installation Progress screen appears, and a progress bar indicates the status of the installation process.

12. Click **Next**.

13. When the Installation Complete screen appears, click **Finish**.

    The installer exits.

Installing the ATE in Silent Mode

This section describes how to install the ATE in silent mode on all platforms.

Use silent mode for installing duplicate installations on multiple machines. You do this by creating and using the **response.rsp** configuration file, and then specifying it as a parameter during a silent mode installation. When silent mode is used, the installation program does not display any options during the installation process.

To install the ATE in silent mode:

1. Log in to the target system.

2. Download the Services Gatekeeper ATE installer from the Oracle software delivery website:

   https://edelivery.oracle.com/

3. Create a **response.rsp** file in a text editor.

4. Add the following contents to the file:

```
[ENGINE]

#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

#The oracle home location. This can be an existing Oracle Home or a new Oracle
Home
ORACLE_HOME=Middleware_home

#Set this variable value to the Installation Type selected. For example, ATE.
INSTALL_TYPE=ATE
```

5. Save the file in the directory where you downloaded the ATE package.

6. From the directory where you downloaded the ATE package, enter:

```
java -jar ocsg_sdk_generic.jar -silent -responseFile ResponseFile
```

   where *ResponseFile* is the full path and name of the Response File. For example, **/home/use/bin/response.rsp**.

The installation proceeds with no prompts.

Where to Go from Here

Perform the tasks described in "Services Gatekeeper Post-Installation Tasks".

11

Upgrading Services Gatekeeper

This chapter describes how to upgrade Oracle Communications Services Gatekeeper from versions 5.0, 5.0.0.1, and 5.1 to version 6.0. Upgrades are supported on the Linux, Solaris, and Windows operating systems.

For more information about supported operating systems, see "Services Gatekeeper System Requirements".

About Upgrading Services Gatekeeper

During the upgrade process, each server in the domain, one at a time, is stopped, upgraded to the new version, and then re-started. This process upgrades the WebLogic Server and the Services Gatekeeper core services, but leaves all communication services unchanged.

After all servers have been upgraded, the communication services in use need to be upgraded. You do this by using in-production redeployment, which is a WebLogic Server feature that enables the communication services to be upgraded without any traffic interruption.

After the upgrade, the security identity of Services Gatekeeper is the same as it was before the upgrade.

The high-level workflow is:

1. Gracefully shut down each Services Gatekeeper server.
2. Upgrade each server. See "Upgrading Servers" for details.
3. Deploy new Services Gatekeeper applications.
4. Verify that new traffic is processed.

You should always upgrade the servers in this order:

1. Administration server
2. First Access Tier server
3. First Network Tier server
4. Second Access Tier server
5. Second Network Tier server

Oracle strongly recommends that you back up configuration data prior to the upgrade. See “Managing, Backing Up, and Restoring Services Gatekeeper” in *Services Gatekeeper System Administrator’s Guide* for more information.

Upgrade Restrictions

The following restrictions apply when upgrading Services Gatekeeper:

- Do not make configuration changes during the upgrade process until all of the servers in the cluster have been upgraded. This is especially important for new configuration options. Services Gatekeeper servers ignore settings that are not understood, and the local configuration file may not be updated properly.
- During the upgrade, the location of the old Services Gatekeeper installation and the location of the new Services Gatekeeper installation must be in two different directories.

Placeholders Used in This Chapter

In addition to the placeholders described in "Placeholders Used in this Guide", Table 11–1 describes the directories and values that are specific to upgrading.

Table 11–1 Upgrade-Specific Placeholders

Placeholder	Description
new_Middleware_home	The new Middleware home directory is the directory under which you install Services Gatekeeper 6.0. Middleware home is the repository for common files that are used by Oracle Communications service delivery products such as Services Gatekeeper, WebLogic Server, and Java Development Kit.
new_Services_ Gatekeeper_home	The directory in which the new version of the Services Gatekeeper software is installed. By default, this is *new_Middleware_home***/ocsg**.
old_version	The two-digit version number, without periods, of the existing Services Gatekeeper version to be upgraded. For example, **51** represents version 5.1.
new_version	The two-digit version number, without periods, of the new Services Gatekeeper version to which you are upgrading. For example, **60** represents version 6.0.
new_Domain_home	The directory in which you create the new Services Gatekeeper domain. By default, this is a subdirectory of the *old_Middleware_ home***/user_projects/domains** directory.

Upgrading Servers

To upgrade a server, perform the following on each machine that hosts your Administration Server, Access Tier server, and Network Tier server:

1. If your old version of Services Gatekeeper includes Services Gatekeeper Reports, undeploy your Services Gatekeeper Reports application EAR file (**edr_to_ analytic.ear**), which is located in the *new_Middleware_home***/ocsg/applications** directory.

   For more information about using the Administration Console to undeploy applications, see "Deploying and Undeploying Communication Services and Plug-ins" in *Services Gatekeeper System Administrator's Guide*.

2. Stop the server gracefully so that all processing requests are completed before the shutdown begins.

   For information about how to stop a server by using the Administration Console, see "Starting, Stopping, and Administering Servers" in *Services Gatekeeper System Administrator's Guide*.

Note: In high-volume traffic situations, you may encounter an excessively long shutdown period. Set a **Graceful Shutdown Timeout** or enable the **Ignore Sessions During Shutdown** option to remedy that behavior.

For information about controlling graceful shutdowns, see the section about controlling graceful shutdowns in *Oracle WebLogic Server Administration Console Online Help* at

http://docs.oracle.com/cd/E24329_01/apirefs.1211/e24401/taskhelp/startstop/ControlGracefulShutdowns.html

3. Install JDK 1.7.0_55 or higher on your system and set the JAVA_HOME environment variable.

   Download the JDK from the Java page on the Oracle Technology Network website at:

   http://www.oracle.com/technetwork/java/index.html

4. Install the new version of Services Gatekeeper in the *new_Middleware_home* directory. Do not configure a domain.

   During the upgrade, the location of the old installation and the location of the new installation must be in two different directories.

   See "Installing Services Gatekeeper" for details.

5. If you are upgrading Reports, perform the tasks described in "Upgrading Services Gatekeeper Reports".

6. (Administration server only) Go to the *new_Middleware_home*/**wlserver/common/templates/scripts/upgrade** directory.

   Note: Only perform steps 7 through 10 once on each of your administration servers.

7. (Administration server only) Unzip the **migration.zip** archive into the **upgrade** directory.

   The **migration** subdirectory is created.

8. (Administration server only) Go to the *new_Middleware_home*/**wlserver/common/templates/scripts/upgrade/migration/***old_version* directory.

9. (Administration server only) Change the permissions for the *old_version* directory:

   ```
   chmod +x oldversion
   ```

10. (Administration server only) At a command prompt, enter one of the following:

    - On Solaris and Linux:

      ```
      sh runConfigurationMigration.sh DatabaseType DatabaseHost DatabasePort
      DatabaseName DatabaseUsername DatabasePassword
      ```

    - On Windows:

      ```
      runConfigurationMigration.bat DatabaseType DatabaseHost DatabasePort
      ```

```
DatabaseName DatabaseUsername DatabasePassword
```

where:

- *DatabaseType* is either **Oracle** or **MySQL**.
- *DatabaseHost* is the host name of the database server.
- *DatabasePort* is the port number through which the database host listens.
- *DatabaseName* is the name of the database or service hosting the Services Gatekeeper data.
- *DatabaseUsername* is the user name that will access the Services Gatekeeper database.
- *DatabasePassword* is the password for the database user.

11. Go to the *new_Middleware_home***/wlserver/common/templates/scripts/upgrade** directory, and open the **undeploy.py** file in a text editor.
12. Edit the following parameters:
    - **AdminServerListenAddress**: The IP address of the Administration Server.
    - **AdminServerListenPort**: The listen port of the Administration Server.
    - **adminName**: The main administrator user name.
    - **adminPassword**: The main administrator password.
    - **serverName**: The name of the server that is hosting the Administration Server.
13. Save and close the file.
14. Ensure that the Administration Server is running.

    For more information, see "Starting and Stopping Servers" in *Services Gatekeeper System Administrator's Guide.*
15. From the *new_Middleware_home***/wlserver/common/templates/scripts/upgrade** directory, enter the following at the command line:

    ```
    sh new_Middlware_home/wlserver/common/bin/wlst.sh undeploy.py
    ```

16. Shut down all Administration Servers, Access Tier servers, and Network Tier servers.

    For more information, see "Starting and Stopping Servers" in *Services Gatekeeper System Administrator's Guide.*
17. To upgrade the Administration Server, perform the following on the system hosting your Administration Server:
    a. Ensure that you are using the correct version of the JDK and that the JAVA_HOME environment variable is set correctly.
    b. Go to the *new_Middleware_home***/wlserver/common/templates/scripts/upgrade** directory, and open the **build.properties** file in a text editor.
    c. Edit the following parameters:
       - **server.name**: The name of the Administration Server.
       - **adminurl**: The address of the Administration Server using the following format:

         ```
         URIscheme://IPaddress:Port
         ```

For example:

```
t3://10.111.22.33:7001
```

- **username**: The main administrator user name.
- **password**: The main administrator password.
- **admin.host**: The name of the server that is hosting the Administration Server.
- **admin.port**: The listen port of the Administration Server.
- **production.mode**: Set this to **true** for production systems and to **false** for demonstration systems.
- **domain51.home**: The directory in which your old Services Gatekeeper domain resides.
- **domain51.name**: The name of your old Services Gatekeeper domain.
- **bea51.home**: The *old_Middleware_home* directory.
- **wlsold.home**: The directory in which old Services Gatekeeper release installed WebLogic Server.
- **bea60.home**: The *new_Middleware_home* directory.
- **wlsnew.home**: The directory in which Services Gatekeeper 6.0 installed WebLogic Server.
- **ocsg.home**: The directory in which Services Gatekeeper 6.0 is installed.

d. Save and close the **build.properties** file.

e. At a command prompt, enter the following:

```
ant upgrade
```

f. Restart the Administration Server.

18. To upgrade the Access Tier, perform the following on the Access Tier server:

Note: If your Access Tier server and Administration Server are installed in the same location, skip this step.

---

a. Set the necessary environment variables.

Windows: Run the script *new_Middleware_home***wlserver\common\bin\commEnv.cmd**

Solaris and Linux: Source the script *new_Middleware_home*/**wlserver/common/bin/commEnv.sh**

b. Go to the *new_Middleware_home*/**wlserver/common/templates/scripts/upgrade** directory and open the **build.properties** file in a text editor.

c. Edit the following parameters:

- **server.name**: The name of the Administration Server.
- **adminurl**: The address of the Administration Server using the following format:

```
URIscheme://IPaddress:Port
```

For example:

```
t3://10.111.22.33:7001
```

- **username**: The main administrator user name.
- **password**: The main administrator password.
- **admin.host**: The name of the server that is hosting the Administration Server.
- **admin.port**: The listen port of the Administration Server.
- **production.mode**: Set this to **true** for production systems and to **false** for demonstration systems.
- **domain51.home**: The directory in which the Services Gatekeeper 5.1 domain resides (*old_Domain_home*).
- **domain51.name**: The name of your Services Gatekeeper 5.1 domain.
- **bea51.home**: The *old_Middleware_home* directory.
- **wlsold.home**: The directory in which Services Gatekeeper 5.1 installed WebLogic Server.
- **bea60.home**: The *new_Middleware_home* directory.
- **wlsnew.home**: The directory in which Services Gatekeeper 6.0 installed WebLogic Server.
- **ocsg.home**: The directory in which Services Gatekeeper 6.0 is installed.

d. Save and close the **build.properties** file.

e. At a command prompt, enter the following:

```
ant upgrade
```

f. Restart the Access Tier server.

19. To upgrade the Network Tier, perform the following on the Network Tier server:

> **Note:** If your Network Tier and Administration Server are installed in the same location, skip this step.

a. Set the necessary environment variables.

Windows: Run the script *new_Middleware_home***wlserver\common\bin\commEnv.cmd**

Solaris and Linux: Source the script *new_Middleware_home*/**wlserver/common/bin/commEnv.sh**

b. Go to the *new_Middleware_home*/**wlserver/common/templates/scripts/upgrade** directory and open the **build.properties** file in a text editor.

c. Edit the following parameters:

- **server.name**: The name of the Administration Server.
- **adminurl**: The address of the Administration Server using the following format:

```
URIscheme://IPaddress:Port
```

For example:

```
t3://10.111.22.33:7001
```

- **username**: The main administrator user name.
- **password**: The main administrator password.
- **admin.host**: The name of the server that is hosting the Administration Server.
- **admin.port**: The listen port of the Administration Server.
- **production.mode**: Set this to **true** for production systems and to **false** for demonstration systems.
- **domain51.home**: The directory in which the Services Gatekeeper 5.1 domain resides (*old_Domain_home*).
- **domain51.name**: The name of your Services Gatekeeper 5.1 domain.
- **bea51.home**: The *old_Middleware_home* directory.
- **wlsold.home**: The directory in which Services Gatekeeper 5.1 installed WebLogic Server.
- **bea60.home**: The *new_Middleware_home* directory.
- **wlsnew.home**: The directory in which Services Gatekeeper 6.0 installed WebLogic Server.
- **ocsg.home**: The directory in which Services Gatekeeper 6.0 is installed.

d. Save and close the **build.properties** file.

e. At a command prompt, enter the following:

```
ant upgrade
```

f. Restart the Network Tier server.

20. Redeploy the **rest.jar** application, which is located in the *new_Middleware_home*/**ocsg/applications** directory.

21. Stop the Administration Server.

22. Go to the *old_domain_home*/**config** directory and open the **config.xml** file in a text editor.

23. Set the **<source-path>** parameter to *new_Middleware_home*/**ocsg/applications/rest.jar**. For example:

```
<library>
     <name>rest-core#1.0@1.0.0.0</name>
     <target>WLNG_NT_Cluster,WLNG_AT_Cluster</target>
     <module-type xsi:nil="true"></module-type>
     <source-path>${OCSG6.0_Home}/ocsg/applications/rest.jar</source-path>
     <security-dd-model>DDOnly</security-dd-model>
</library>
```

24. Save and close the **config.xml** file.

25. (Complete steps 25 through 29 if you use Node Manager) Open the *new_Middleware_home*/**wlserver/server/bin/startNodeManager.sh** file in a text editor.

26. Add this line to the JAVA_OPTIONS:

```
JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.security.egd=file:/dev/./urandom"
```

27. Copy the *old_Middleware_home***/welserver_10.3/common/nodemanager** directory to *new_Middleware_home***/oracle_common/common**.
28. Delete all files in the new *new_Middleware_home***/oracle_common/common/nodemanager** directory except **nodemanager.domains** and **nodemanager.properties**.
29. Start Node Manager on all servers by running this script:

    ```
    new_Middleware_home/wlserver/server/bin/startNodeManager.sh
    ```

30. Restart your servers in the following order: Administration Server, then first Access Tier server, then second Access Tier server, then first Network Tier server, and then second Network Tier server.
31. Redeploy the **pubsub-1.0.war** application, which is located in the *Middleware_home***/wlserver/common/deployable-libraries/** directory.
32. Stop the Administration Server.
33. Go to the *old_domain_home***/config** directory and open the **config.xml** file in a text editor.
34. Replace the following text:

    ```
    <library>
         <name>pubsub#1.0@1.7.0.0</name>
         <target>WLNG_AT_Cluster</target>
         <module-type>war</module-type>
         <source-path>${OCSG5.1_HOME}/wlserver_
    10.3/common/deployable-libraries/pubsub-1.0.war</source-path>
         <security-dd-model>DDOnly</security-dd-model>
    </library>
    ```

    with this text:

    ```
    <library>
         <name>pubsub#1.0@3.0.0.0</name>
         <target>WLNG_AT_Cluster</target>
         <module-type>war</module-type>
         <source-path>${OCSG6.0_
    HOME}/wlserver/common/deployable-libraries/pubsub-1.0.war</source-path>
         <security-dd-model>DDOnly</security-dd-model>
         <staging-mode xsi:nil="true"></staging-mode>
         <plan-staging-mode xsi:nil="true"></plan-staging-mode>
         <cache-in-app-directory>false</cache-in-app-directory>
    </library>
    ```

35. Save and close the **config.xml** file.
36. Restart your Administration Server, then your first Access Tier server, and then your second Access Tier server.
37. Follow the procedure in "Deploying New Services Gatekeeper Applications".

Deploying New Services Gatekeeper Applications

After upgrading, you must undeploy all deprecated applications and redeploy the new Services Gatekeeper applications. You do this by using the hitless upgrade procedure. For more information about hitless upgrades, see the following:

- "Upgrading and Redeploying Communication Services and Service Interceptors" in *Services Gatekeeper System Administrator's Guide*
- "Redeploying Applications in a Production Environment" in *Oracle Fusion Middleware Deploying Applications to Oracle WebLogic Server*.

To deploy the new Services Gatekeeper applications:

1. Undeploy the following deprecated application EAR files:
   - **wlng_nt_oauth2.ear**
   - **wlng_nt_portal.ear**
2. Deploy the new Portal Server, Parlay, and XQoS application EARs files, which are located in the *new_Middleware_home***/ocsg/applications** directory:
   - **wlng_nt_oauth2.ear**
   - **wlng_at_qos_px40.ear**
   - **wlng_at_rest_portal_service.ear**
   - **oracle.sdp.daf.externalaction-6.0.0.0.jar** (must be named "DafExternalActions" when deployed)
   - **wlng_nt_portal.ear**
   - **daf-multitier-at.ear** (for cluster implementations only)
   - **daf-multitier-nt.ear** (for cluster implementations only)
   - **daf.war** (for standalone implementations only)
3. Redeploy the Services Gatekeeper 6.0 communication services application EAR files, which are located in the *new_Middleware_home***/ocsg/applications/** directory:
   - **wlng_nt_qos.ear**
   - **wlng_nt_session.ear**
   - **wlng_nt_call_notification_px21.ear**
   - **wlng_nt_multimedia_messaging_px21.ear**
   - **wlng_nt_presence_px21.ear**
   - **wlng_nt_sms_px21.ear**
   - **wlng_nt_terminal_location_px21.ear**
   - **wlng_nt_device_capabilities_px30.ear**
   - **wlng_nt_terminal_status_px21.ear**
   - **wlng_nt_third_party_call_px21.ear**
   - **wlng_nt_subscriber_profile_ews.ear**
   - **wlng_nt_push_message_ews.ear**
   - **wlng_nt_multimedia_messaging_mm7.ear**
   - **wlng_nt_native_smpp_sms.ear**
   - **wlng_nt_payment_px30.ear**
   - **wlng_nt_address_list_px30.ear**
   - **wlng_nt_acr_px21.ear**
   - **wlng_at_portal_service.ear**

- **wlng_at_acr_parlay_rest.ear**
- **wlng_at_address_list_px30.ear**
- **wlng_at_addresslist_parlay_rest.ear**
- **wlng_at_oauth2.ear**
- **wlng_at_session.ear**
- **wlng_at_callable_policy.ear**
- **wlng_at_call_notification_px21.ear**
- **wlng_at_multimedia_messaging_px21.ear**
- **wlng_at_presence_px21.ear**
- **wlng_at_sms_px21.ear**
- **wlng_at_terminal_location_px21.ear**
- **wlng_at_device_capabilities_px30.ear**
- **wlng_at_terminal_status_px21.ear**
- **wlng_at_third_party_call_px21.ear**
- **wlng_at_subscriber_profile_ews.ear**
- **wlng_at_push_message_ews.ear**
- **wlng_at_multimedia_messaging_mm7.ear**
- **wlng_at_payment_px30.ear**
- **interceptors.ear**
- **xparam_interceptors.ear**
- **wlng_at_payment_parlay_rest.ear**
- **wlng_at_sms_parlay_rest.ear**
- **wlng_at_terminallocation_parlay_rest.ear**
- **wlng_at_multimedia_messaging_parlay_rest.ear**
- **wlng_prm.ear**
- **wlng_nt_native_ucp_sms.ear**
- **wlng_at_qos_rest.ear**

4. Redeploy the new Reports application EAR file, which is located in the *new_Middleware_home*/**ocsg/applications** directory.
   - **edr_to_analytic.ear**
5. Reconfigure your Services Gatekeeper Reports.

   For more information, see "Managing StatisticService" in *Services Gatekeeper System Administrator's Guide*.

Cleaning Up Files After Upgrading

The general process for removing the old Services Gatekeeper files after upgrading includes:

1. Making a backup copy of the old Services Gatekeeper *middleware_home* directory and its subdirectories
2. Removing the contents of the old *middleware_home* directory *except for the domain_home directories if you locate them under middleware_home*. You can safely remove everything under the old *middleware_home* except for the *domain_home* and its subdirectories. If your *domain_home* is not under *middleware_home* you can safely just remove everything in *middelware_home*.
3. Starting the new Services Gatekeeper servers to ensure that they work correctly.
4. Then you can remove the backup copy of the old Services Gatekeeper implementation.

Upgrading Services Gatekeeper Reports

You upgrade Services Gatekeeper Reports by upgrading the reports database schema and then deploying the new repository and catalog files.

To upgrade Services Gatekeeper Reports:

1. Go to the *Middleware_home*/**wlserver/common/templates/scripts/upgrade** directory.
2. Unzip the **analytics_migration.zip** archive into the **upgrade** directory.

   The **analytics_migration** directory is created.
3. Go to the *Middleware_home*/**wlserver/common/templates/scripts/upgrade/analytics_migration** directory.
4. At a command prompt, enter one of the following:
   - On Solaris and Linux:

     ```
     sh runConfigurationMigration.sh DatabaseHost DatabasePort DatabaseName DatabaseUsername DatabasePassword
     ```

   - On Windows:

     ```
     runConfigurationMigration.bat DatabaseHost DatabasePort DatabaseName DatabaseUsername DatabasePassword
     ```

   where:

   - *DatabaseHost* is the host name of the database server to be used for reports data.
   - *DatabasePort* is the port number through which the reports database host listens.
   - *DatabaseName* is the name of the database or service hosting the reports data.
   - *DatabaseUsername* is the user name that will access the reports database.
   - *DatabasePassword* is the password for the database user.

   Your reports database schema is now upgraded.
5. Start the Oracle Business Intelligence Administration Tool.

   For more information about starting and using the Oracle Business Intelligence Administration Tool, see "About the Oracle BI Administration Tool" in *Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.

6. In the Oracle Business Intelligence Administration Tool, open the *Middleware_home*/**ocsg/ext/analytics/edr.rpd** file.
7. Modify the repository file's **orcl** and **blockInit** database connection, user name, and password properties to reference your database.

   For instructions about configuring RPD files, including changing the password and setting database connection information, see "Importing Metadata and Working with Data Sources" in *Oracle Fusion Middleware Metadata Repository Builder's Guide for Oracle Business Intelligence Enterprise Edition*.
8. Transfer the **edr.rpd** file to the machine hosting your Oracle Business Intelligence installation.
9. Copy the **catalog.zip** archive from the *Middleware_home*/**wlserver/common/templates/scripts/upgrade/analytics_migration** directory to the machine hosting your Oracle Business Intelligence installation.
10. Unzip the **catalog.zip** archive into the *Oracle_instance*/**bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog/edr6** directory.
11. Redeploy the repository file and catalog file:
    a. Login to the Fusion Middleware Control Console.
    b. In the Navigator, click **Farm_bifoundation_domain**, expand **Business Intelligence**, and then expand **coreapplication**.
    c. Click the **Deployment** tab and then click the **Repository** tab.
    d. Specify the repository file (**edr.rpd**) location and password.
    e. Specify the catalog location as *Oracle_instance*/**bifoundation/OracleBIPresentationServicesComponent/coreapplication_obips1/catalog/edr6**.
    f. Click **Activate Changes**.
    g. Click **Restart**.

    For more information, see "Using Fusion Middleware Control to Upload a Repository and Set the Oracle BI Presentation Catalog Location" in *Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition*.

Upgrade Troubleshooting

This section provides remedies for common problems that occur after a Services Gatekeeper upgrade.

A Network Tier Server Cannot Rejoin Its Coherence Cluster

New versions of Services Gatekeeper may upgrade the Oracle Coherence version. Because of that, sometimes the upgraded server cannot join servers running the earlier version because of the version mismatch. To fix this issue:

1. Edit the script *new_Middleware_home*/**wlserver/common/templates/scripts/upgrade/configCoherence.py** and update the following variables:
   - ADMIN_USER_NAME: The WebLogic administrator user name.

- ADMIN_PASSWORD: The WebLogic administrator password.
- ADMIN_URL: The WebLogic administration console URL.
- FIRST_TIME: Set this to **true** if this is the first Network Tier server you are upgrading; **false** otherwise.

2. Run the script using the following command:

```
# . ../../../bin/wlst.sh configCoherence.py
```

A Network Tier Server Cannot Rejoin Its Services Gatekeeper Cluster

Sometimes an upgraded Services Gatekeeper has a different OAuth 2.0 EBJ home instance from other Network Tier servers and is not be able to join the cluster. To fix this issue:

1. Start the Network Tier server's Administration Console:

   http://*server_address*:*port*/console

   Note: The default Administration Console port is 7001.

2. In the **Change Center** panel, click **Lock & Edit**.
3. In the **Domain Structure** panel, select your Services Gatekeeper domain and then select **Deployments**.
4. In the **Summary of Deployments** pane, select **wlng_nt_outh2** and then select the **Targets** tab.
5. Select **wlng_nt_oauth2**, and click **Change Targets**.
6. Under Clusters, select **Part of the cluster**, and deselect the server that cannot join the cluster. Click **Yes**.
7. In the **Change Center**, click **Activate Changes**.
8. Restart the other Network Tier servers in the cluster.
9. Following the same procedure above, reset the **wlng_nt_oauth2** targets to **All servers in the cluster**, and click **Yes**.
10. Restart the server that could not rejoin its cluster.

Administration Console Pages are Not Displayed Properly

After the upgrade, the pages in the Administration Console may not display properly. If this occurs, delete the browser's cache and cookies and restart the Administration Console.

12

Patch Management of Services Gatekeeper Systems

This chapter describes how you can manage Oracle Communications Services Gatekeeper patches to fix issues or improve the system.

If you are planning to upgrade your Services Gatekeeper system, use the information in "Upgrading Services Gatekeeper".

About Services Gatekeeper Patch Releases

You can develop and maintain a strategy to handle the installation of patch releases so that your customers experience a seamless transition.

Types of Patch Releases

Oracle Communications distributes the following types of patch releases for Services Gatekeeper to resolve issues, to resolve any perceived vulnerability in the software, or to improve its overall performance:

- Patch Set. See "About Patch Sets".
- Debug patch. See "About Debug Patches".
- Temporary fix. See "About Temporary Fixes".

About Patch Sets

A Patch Set is the most comprehensive patch release. It contains the accumulated resolutions and updates in Service Gatekeeper from the time of the last general release up to the current Patch Set release.

Services Gatekeeper 6.0 Patch Sets use the release numbering scheme 6.0.0.*x*, where *x* is the Patch Set number. For example, the first Patch Set for Services Gatekeeper 6.0 would be Services Gatekeeper 6.0.0.1.

Note: Oracle recommends that you stay up-to-date by installing Patch Sets as soon as they become available.

About Debug Patches

A debug patch is used to troubleshoot an ongoing issue in your Services Gatekeeper system.

A debug patch represents a concerted attempt by you and Oracle Technical Support to fix an issue in your Services Gatekeeper system. Oracle Technical Support uses debug patches as a tool to extract better data from your Services Gatekeeper system as a way of resolving the issue. Consequently, the debug patch may not resolve the issue, and additional patches may be required.

Because debug patches address a singular issue, Services Gatekeeper numbers them as v1, v2, v3, and so on. Each subsequent version replaces the prior version of the debug patch.

About Temporary Fixes

Temporary fixes are tailored to solve an issue in your Services Gatekeeper system. They are sent to you as urgent, time-sensitive or critical corrections that solve an issue you are experiencing instead of waiting to set up the fix as part of a scheduled Services Gatekeeper Patch Set.

You may have to install additional patches to make the temporary fix work.

Because each temporary fix addresses a single issue, Services Gatekeeper numbers the fixes as v1, v2, v3, and so on. Each subsequent version replaces the prior version of the temporary fix.

Finding Your Current Patch Level

See "Finding the Current Patch Level of Your Services Gatekeeper System" in *Services Gatekeeper Administrator's Guide* to find your current patch level.

About Patch Content

By default, every patch contains the following items:

- A README file

  The README file for a patch release describes how to install the patch. Additionally, in case you encounter problems while applying the patch, the README describes how you can revert to your current setup by rolling back the patch.

- Updates to Services Gatekeeper

  These consist of fixes or debug changes.

At times, the patch may contain a subdirectory named **custom**. Services Gatekeeper places the following items in this directory:

- Additional documentation resources

  For example, the patch may contain the description of a specific fix detailing what additional configuration settings may be required to utilize the fix.

- Manual patching steps

  The patch may target a resource you may have modified, such as startup scripts. Services Gatekeeper provides manual patching steps to assert that your modifications are not lost.

About Patch Management In Clustered Environments

If your Services Gatekeeper system operates in a clustered environment, review the README file that accompanies the patch. Ensure that you apply the patch to all of the servers. Then perform a rolling restart unless otherwise stated in the README file.

About OPatch

OPatch is an Oracle-supplied Java-based utility that supports the following tasks:

- Applying a patch
- Rolling back a patch to a previous version
- Listing the installed patches
- Detecting a conflict when applying a patch after previous patches have been applied. It also suggests the best options to resolve a conflict

OPatch requires installation of the Oracle Universal Installer (OUI). It is platform-independent and runs on all supported operating systems.

For more information, see "Patching Oracle Fusion Middleware with Oracle OPatch" in *Oracle Fusion Middleware Patching Guide*.

Requirements for OPatch

Before you run OPatch, perform the prerequisite checks for OPatch as described in *Oracle Fusion Middleware Patching with OPatch*. For example, the ORACLE_HOME environment variable must point to a valid *Middleware_home* directory and match the value used during Services Gatekeeper installation.

For the latest information about the OPatch utility, the JRE versions, or the Java commands for Windows, Solaris, and Linux, or to check for updates and get the latest versions, go to My Oracle Support at:

`https://support.oracle.com/`

Managing a Patch Release Installation Process

Managing a patch release installation consists of the following tasks:

1. Preparing to Install the Patch
2. Stopping All WebLogic Servers
3. Installing the Patch
4. Completing Patch Installation

If you encounter any issues in any of these steps, see "Troubleshooting".

Preparing to Install the Patch

Complete the following tasks before you install the patch:

1. Verifying the Oracle Universal Installer Inventory
2. Creating a Backup of Your Current Services Gatekeeper Installation
3. Checking Your Environment Variables
4. Creating a Location for the Patch

Verifying the Oracle Universal Installer Inventory

To apply patches successfully, OPatch needs access to a valid OUI. Validate the OUI inventory with the following command:

```
opatch lsinventory
```

For more information, see "OPatch Utility Reference".

> **Caution:** If the **lsinventory** command errors out, do not proceed further with the patch attempt.
>
> Contact Oracle Technical Support to validate and verify the inventory setup.

Creating a Backup of Your Current Services Gatekeeper Installation

Before you start any patch operation, back up the contents of the *Middleware_home* directory. You can back up the contents of *Middleware_home* by using your preferred method. Use any of the following methods to compress the *Middleware_home* contents:

- zip
- cp -r
- tar
- cpio

Checking Your Environment Variables

The patch installation process uses the OPatch and Zip software. Ensure that your system can find and use the software by setting the following environment variables:

- Set your PATH environment variable to include the path to your *Middleware_home*/**OPatch** directory and to your Zip software.
- Set your ORACLE_HOME environment variable to your *Middleware_home* directory.

To confirm that your system can find the OPatch and Zip software, enter the following at a command prompt:

```
which opatch
which unzip
```

> **Note:** If your system cannot find the path to the software, double-check that your environment variables are set correctly.

Creating a Location for the Patch

Create a location for storing the unzipped patch. This chapter refers to the location as *Patch_top*.

Stopping All WebLogic Servers

At this point, you should have completed the necessary checks, backed up your current Services Gatekeeper system, and created a location for the patch files.

Check the README file to determine whether you must stop all servers in your Services Gatekeeper system. The README file will state whether the patch requires you to stop your servers prior to installing the patch.

Installing the Patch

To install the patch:

1. Log in to the target system.
2. Download the patch from the My Oracle Support website to a temporary directory:

   https://support.oracle.com/
3. Change to the directory where you downloaded the patch.
4. Unzip the patch archive (*PatchName*.**zip**) into the *Patch_top* directory.

   The *PatchName* subdirectory is created.

   Note: Ensure that the *PatchName*.**zip** file is not located inside the *Patch_top* directory.
5. Go to the *Patch_top*/*PatchName* directory.
6. Run the OPatch utility by entering the following at a command prompt:

   opatch apply *Patch_top*/*PatchName*

   OPatch validates the patch and makes sure there are no conflicts with the software already installed in *Middleware_home* before applying the patch to your Services Gatekeeper system.

   For more information, see "OPatch Utility Reference" and "Dealing with Conflicts When You Run the Apply Command".
7. Verify that the patch installed successfully by running the following command:

   opatch lsinventory

   For more information, see "OPatch Utility Reference".

Completing Patch Installation

At this point, you have installed the patch successfully and verified the contents of the *Middleware_home* directory.

Check the README file to determine if you must restart all servers in your Services Gatekeeper system. The README file will state whether the patch requires you to restart your servers or to redeploy a specific module or application.

Troubleshooting

OPatch is reliable and protects *Middleware_home* and the inventory. It can bring back the contents of the *Middleware_home* directory to a stable state from patch application failures. It can also easily detect patch conflicts.

OPatch logs information to a **.log** file. Here is an example entry:

```
Log file location : /home/oracle_
TEST/product/11.1.0/db1/cfgtoollogs/opatch/opatch-yyyy_month_dd_HH-MM-SS-IST_
Wed.log
```

If you encountered errors while installing a patch and you need assistance from Oracle Technical Support, be sure to provide the associated log file together with the patch command you used to install the patch.

Uninstalling the Patch

If you experience any problems after installing a patch, remove the patch.

To uninstall the patch:

1. Follow the same prerequisites or pre-install steps you took when you completed the following:
   - Preparing to Install the Patch
   - Stopping All WebLogic Servers
2. Roll back the patch with the following command:

   ```
   opatch rollback -id PatchNumber
   ```

   where *PatchNumber* is the patch number. For more information, see "OPatch Utility Reference".

If you need further assistance, contact Oracle Technical Support with the required information.

OPatch Utility Reference

By default, the OPatch utility is located in the *Middleware_home*/**OPatch** directory. The syntax for running the OPatch utility from the valid directory is shown below:

```
opatch [-help] [-report] [command]
```

where:

- **help** lists the commands and options supported by the utility.

  Use the **-help** parameter together with a command to view detailed information for the OPatch command. For example:

  ```
  opatch apply -help
  ```

- **report** prints the actions without executing the command.
- *command* is one of these OPatch commands:
  - **apply** [*Patch_top*/*PatchName*]

    This command applies the patch to the software located in *Middleware_home*, where *Patch_top*/*PatchName* is the directory that contains the patch contents. (When you unzip the patch archive to *Patch_top*, it creates a *PatchName* subdirectory that includes all of the patch contents.)

    For the command to work properly, the ORACLE_HOME environment variable must be set to *Middleware_home*. See "Dealing with Conflicts When You Run the Apply Command".

  - **lsinventory**

    This command displays your system's OPatch and OUI versions and directories, and lists the patches currently installed in *Middleware_home*. The following shows sample output for the **lsinventory** command:

    ```
    ---------------------------------------------------------------------
    Oracle Interim Patch Installer version 13.2.0.0.0
    Copyright (c) 2014, Oracle Corporation. All rights reserved.

    Oracle Home          : Middleware_home
    ```

```
Central Inventory    : /export/oraInventory
   from              : Middleware_home/oraInst.loc
OPatch version       : 13.2.0.0.0
OUI Version          : 13.2.0.0.0
Log file location    : Middleware_home/cfgtoollogs/opatch/opatch2014-12-16_
11-16-55AM_1.log

OPatch detects the Middleware Home as "Middleware_home"

--------------------------------------------------------------------------
Interim patches (1):

Patch  19836145      : applied on Tue Dec 16 10:51:13 CST 2014
Unique Patch ID      : 1418034883552
Patch description    : "[Patch Set v6.0.0.0.1] - Patch set zero"
   Created on 8 Dec 2014, 02:34:45 hrs PST8PDT
   Bugs fixed:
     123412
--------------------------------------------------------------------------
```

– **rollback -id** *PatchNumber*

  This command removes the specified patch from the *Middleware_home* directory, where *PatchNumber* is the patch number. You can find the patch number by using the **lsinventory** command. For example, you would use the command **rollback -id 19836145** to roll back the patch shown in the following sample **lsinventory** output:

```
--------------------------------------------------------------------------
Interim patches (1) :

Patch  19836145     : applied on Tue Dec 16 10:51:13 CST 2014
Unique Patch ID:  1418034883552
Patch description:  "[Patch Set v6.0.0.0.1] - Patch set zero"
   Created on 8 Dec 2014, 02:34:45 hrs PST8PDT
   Bugs fixed:
     123412
--------------------------------------------------------------------------
```

For a full list of the OPatch commands and their descriptions, see *Oracle Fusion Middleware Patching with OPatch*.

Dealing with Conflicts When You Run the Apply Command

When you run the OPatch **apply** command, you may encounter the following conflicts:

- Conflict with a patch already applied to the contents of the *Middleware_home* directory.

  In this case, stop the patch installation and contact Oracle Technical Support.

- Conflicts with a subset patch already applied to the contents of the *Middleware_home* directory.

  In this case, continue the installation, as the new patch contains all the fixes from the existing patch. The subset patch will automatically be rolled back prior to the installation of the new patch.

13

Uninstalling Services Gatekeeper

This chapter describes how to uninstall Oracle Communications Services Gatekeeper and its components.

Uninstalling Services Gatekeeper Components in GUI Mode

To uninstall Services Gatekeeper components in GUI mode:

1. Go to the *Middleware_home*/**oui/bin** directory and enter the following in a command window:

   ```
   ./deinstall.sh
   ```

2. If you have multiple Oracle products installed in your *Middleware_home* directory, the Distribution to Uninstall screen appears.

   Perform the following to specify the Oracle product to uninstall:

   a. From the **Select Distribution to Uninstall** list, select the software you want to uninstall. For example, select one of the following:

      Oracle Communications Services Gatekeeper 6.0.0.0.0

      OCSG Platform Test Environment 6.0.0.0.0

      OCSG Application Test Environment 6.0.0.0.0

      OCSG Analytics 6.0.0.0.0

   b. Click **Uninstall**.

3. From the Welcome screen, click **Next**.

   The Deinstallation Summary screen appears.

4. Verify that the list of feature sets to deinstall is correct.

   To save the information to a response file so you can uninstall the components later, click **Save Response File** and specify the name and location of the response file.

5. Click **Deinstall**.

   The Deinstallation Progress screen appears, and a progress bar indicates the status of the uninstall process.

6. When the uninstallation process is complete, click **Next**.

   The Deinstallation Complete screen appears.

7. Click **Finish**.

The uninstaller exits.

Uninstalling Services Gatekeeper Components in Silent Mode

This section describes how to uninstall Services Gatekeeper components in silent mode on all platforms.

Use silent mode to uninstall duplicate installations on multiple machines. You do this by creating and using a **response_uninistall.rsp** configuration file, and then specifying it as a parameter during a silent mode uninstallation. When silent mode is used, the program does not display any options during the uninstall process.

To uninstall Services Gatekeeper components in silent mode:

1. Create a text file on your target system.
2. Add the following contents to your file:

```
[ENGINE]
#DO NOT CHANGE THIS.
Response File Version=1.0.0.0.0

[GENERIC]

#This will be blank when there is nothing to be de-installed in distribution
level
SELECTED_DISTRIBUTION=Oracle Communications Services Gatekeeper~6.0.0.0.0

#The oracle home location. This can be an existing Oracle Home or a new Oracle
Home
ORACLE_HOME=Middleware_home
```

   where SELECTED_DISTRIBUTION is set to the component to uninstall. This parameter is required only if multiple applications are installed in *Middleware_home*. The following list shows the values for Services Gatekeeper components:

   - Oracle Communications Services Gatekeeper~6.0.0.0.0
   - OCSG Application Test Environment~6.0.0.0.0
   - OCSG Platform Test Environment~6.0.0.0.0
   - OCSG Analytics~6.0.0.0.0

3. Save the file with the name **response_uninstall.rsp**.
4. Go to the *Middleware_home***/oui/bin** directory and enter the following in a command window:

   ./deinstall.sh -silent -responseFile *ResponseFile*

   where *ResponseFile* is the full path and name of the **response_uninstall.rsp** file. For example, *Middleware_home***/oui/bin/response_uninstall.rsp**.

   The uninstall process completes with no prompts.

If the uninstall procedure completes successfully, you will see a response similar to the following:

```
Launcher log file is /tmp/OraInstall2014-11-06_01-46-10PM/launcher2014-11-06_
01-46-10PM.log.
Starting Oracle Universal Installer

Checking if CPU speed is above 300 MHz.   Actual 2893.030 MHz    Passed
```

```
Checking swap space: must be greater than 512 MB.   Actual 15826924 MB    Passed
Checking if this platform requires a 64-bit JVM.   Actual 64    Passed (64-bit not
required)
Checking temp space: must be greater than 300 MB.   Actual 136360 MB    Passed


Preparing to launch the Oracle Universal Installer from /tmp/OraInstall2014-11-06_
01-46-10PM
Java HotSpot(TM) 64-Bit Server VM warning: ignoring option MaxPermSize=512m;
support was removed in 8.0
Log: /tmp/OraInstall2014-11-06_01-46-10PM/deinstall2014-11-06_01-46-10PM.log
Setting ORACLE_HOME to /home/oracle/
Copyright (c) 1996, 2015, Oracle and/or its affiliates. All rights reserved.
Starting silent deinstallation...
-----------20%----------40%----------60%----------80%--------100%

The uninstall of Oracle Communications Services Gatekeeper 6.0.0.0.0 completed
successfully.
Logs successfully copied to /export/oraInventory/logs.
```

14

Next Steps

This chapter provides information about initial system administration tasks that you must perform after you have completed all Oracle Communications Services Gatekeeper installation and post-installation tasks.

Configuring Services Gatekeeper

You can now proceed to configuring Services Gatekeeper itself. Instructions are described in the *Services Gatekeeper System Administrator's Guide* and *Services Gatekeeper Portal Developer's Guide*. The following list gives a general outline of the initial tasks you must perform:

- Create administrative user accounts
- Configure Services Gatekeeper container services
- Configure communication services
- Configure connections with OSA/Parlay gateways, as necessary
- Set up and configure web services security and Oracle Access Manager (OAM) (JMX) security
- Configure the Partner Relationship Management interfaces, as necessary
- Configure geographic redundancy, if necessary
- Create service provider and application accounts
- Create service provider and application SLAs
- Create network SLAs