Oracle® Communications Session Delivery Manager

Security Guide

Release 8.0

August 2017

Oracle Communications Session Delivery Manager Security Guide, Release 8.0

Contents

List of Figures

List of Tables

About This Guide

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

Note:

With the introduction of the product plugin service and changes in the SDM product, only the Oracle Communications Session Delivery Manager Documentation Library appears in this section of each SDM guide.

Related Documentation

Table 1 Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	Provides the following administration information: • Implement SDM on your network as a standalone server or high availability (HA) server. • Login to the SDM application, access GUI menus including help, customize the SDM application, and change your password. • Access the product plugin service through the GUI to manage product plugin tasks, including how product plugins are uploaded and installed. • Manage security, faults, and transport layer security certificates for east-west peer SDM server communication, and southbound communication with network function (NF) devices. • Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems. • Monitor SDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics. • Maintain SDM server operations, which includes database backup and database restoration and performing server cluster operations. • Use available SDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the SDM server.
Installation Guide	Provides the following installation information: • Do pre-installation tasks, which include reviewing system requirements, adjusting linux and firewall settings, completing SDM server settings and configuring your NNCentral account for security reasons. • Do the typical installation to perform the minimal configuration required to run the SDM server. • Do the custom installation to perform more advanced configurations including the mail server, cluster management, Route Manager, transport layer security (TLS), and Oracle database configuration.

Table 1 (Cont.) Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Release Notes	Contains information about the administration and software configuration of the SDM feature support new to this release.
Security Guide	Provides the following security guidelines: • Use guidelines to perform a secure installation of SDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines. • Review Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system. • Follow a checklist to securely deploy SDM on your network and maintain security updates.
REST API Guide	Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a network service orchestrator (NSO), to interact with SDM and its supported product plugins.
SOAP API Guide	The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programing model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the SDM server and data structures that are used as input and output parameters for these operations.

1

Session Delivery Manager Application Overview

Oracle Communications Session Delivery Manager is a network element management system that can be accessed through a graphical user interface (GUI), REST API interface, or SOAP API interface.

Once SDM is installed, you can access the following sliders:

> **Note:**
>
> Other sliders, such as the Device Manager, Configuration Manager, Performance Manager, and so on, will not be seen until you install a product plug-in.

- **Device Manager**—Use this slider to configure device groups. The functionality of this slider is dependant on the product plug-in(s) that you have installed.
- **Security Manager**—Use this slider to configure any security privileges that are specific to Oracle Communications Session Delivery Manager and the Oracle Communications Session Delivery Manager product plugin.
- **Fault Manager**—View events, alarms, and trap summary data.

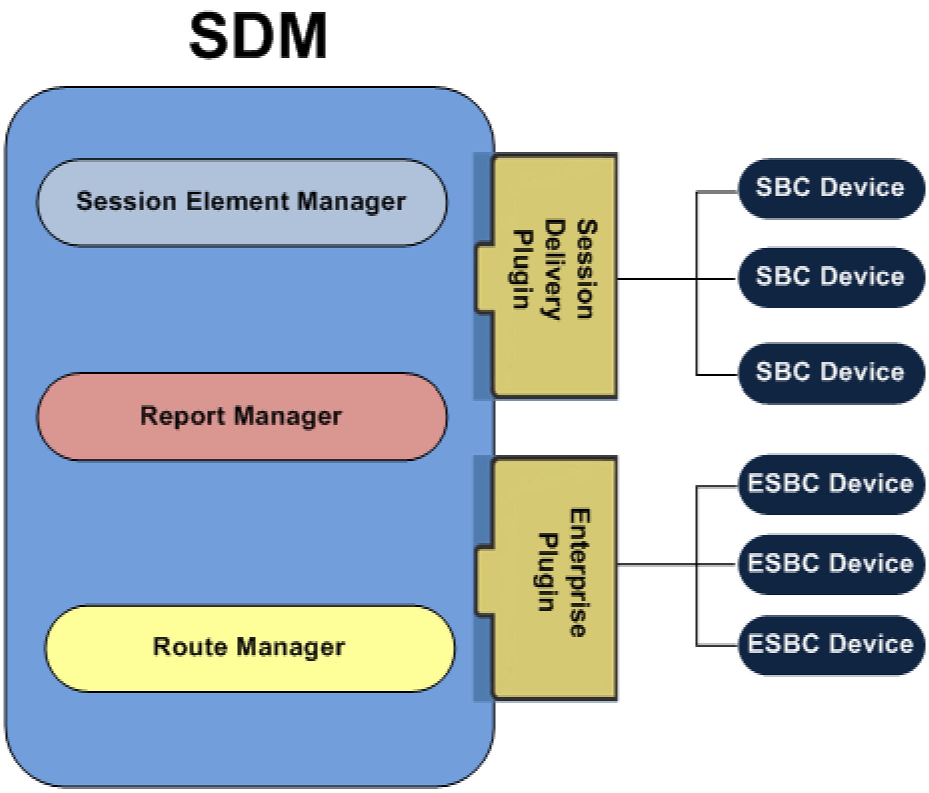
Session Delivery Manager Product Plugin Service

A product plugin is used to activate fault, configuration, accounting, performance, and security (FCAPS) in Oracle Communications Session Delivery Manager. For example, the Session Delivery (SD) product plugin activates Oracle Communications Session Element Manager in SDM for session delivery devices, such as the Oracle Communications Session Border Controller (SBC).

SDM has limited functionality until a plugin is uploaded and installed in SDM. Product functionality activated by the plugin in the SDM GUI is specific to what the plugin supports. For example, if you see a drop-down menu, field or checkbox that cannot be accessed, the plugin does not support this functionality in the GUI.

Use the plugin service in Oracle Communications Session Delivery Manager to install the product plugin, which provides different sliders depending on the instructions contained in the product plugin. For example, the **Dashboard Manager**, **Configuration Manager**, **Performance Manager**, **Report Manager**, and **Route Manager** sliders appear once the SD plug-in is installed. See the product plug-in documentation for more information about supported sliders.

More than one product plugin can be installed on SDM at the same time, and the functionality of the plugin(s) is propagated to other SDM nodes in a clustered environment. The following example shows how the SD and Enterprise product plugins provide their respective devices access to Session Element Manager, Report Manager and Route Manager.


SDM
Session Element Manager
Report Manager
Route Manager
Session Delivery Plugin
Enterprise Plugin
SBC Device
SBC Device
SBC Device
ESBC Device
ESBC Device
ESBC Device

2

Secure Installation Guidelines

This chapter outlines installation options for Oracle Communications Session Delivery Manager, and provides guidelines to install Oracle Communications Session Delivery Manager securely on your server. See your product installation guide for more information.

Secure the Server

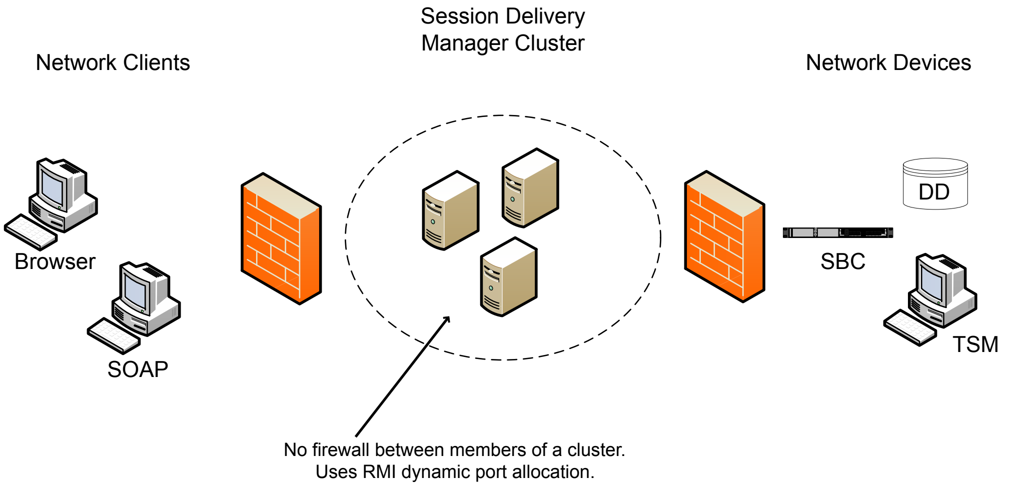
You must secure the server before you install Oracle Communications Session Delivery Manager .

Use the following documents to help secure the server on which Oracle Communications Session Delivery Manager is installed:

- Guide to the Secure Configuration of Red Hat Enterprise Linux 6
- Hardening Tips for the Red Hat Enterprise Linux 6
- Oracle Linux Security Guide for Release 6
- Tips for Hardening an Oracle Linux Server
- CentOS Wiki: OS Protection

Check Firewall Settings

When setting up Oracle Communications Session Delivery Manager (SDM) in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the SDM cluster, and a firewall between the SDM cluster and other devices.


Network Clients
Session Delivery Manager Cluster
Network Devices
Browser
SOAP
DD
SBC
TSM
No firewall between members of a cluster.
Uses RMI dynamic port allocation.

Note:

You cannot have firewalls between the servers in a cluster.

If firewalls exist on either side of the SDM cluster, ensure the ports listed in the following table are open. If your operating system comes with a firewall, you need to apply the same criteria. You must switch off the firewall in your operating system or ensure these ports are available.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
Between SDM Cluster and Network Clients					
8443	TCP	HTTPS	N	Y	Apache port. HTTPS port for client/ server communication.
8080	HTTP	HTTP	N	Y	HTTP port for client/server communication.
Between SDM Cluster and Network Devices					
161	UDP	SNMP	N	Y	SNMP traffic between the SDM server and the device.
162	UDP	SNMP	N	Y	SNMP trap reporting from the device to the SDM server.
22/21	SFTP/FTP				Used for file transfer (such as Route Manager and LRT updates).
8080	HTTP	AMI	N	Y	Used by SDM to communicate with 9200 devices via AMI.
5060	TCP		N	Y	Used for SDM Trunk Manager (SIPTX) to communicate with SP-SBC.
3001/ 3000		ACP/ACLI			Used by SDM to communicate with all versions of the device except for the Acme Packet 9200.
Between SDM Servers in the Cluster					
1098	TCP	RMI	N	Y	RMI Communication between host members in a cluster.
1099	TCP	RMI Lookup	N	Y	RMI registry port. Used for the RMI communication between host members in a cluster.
5701	TCP	Hazelcast	N		Used by Hazelcast communication for distributed data structures, peer-to-peer collective data distribution.
5000/ 5801	TCP	Hazelcast	N	Y	Used by the Hazelcast management console port for the SDM distributed scheduler service.
54327	UDP	Hazelcast	N	Y	Used by Hazelcast for cluster member discovery.
8005	TCP	HTTP	N	Y	Tomcat shutdown port used by the shutdown script. Can be blocked on a firewall because it is local to the SDM server.
8009	TCP	Apache	N	Y	Tomcat port.
9000	TCP	Berkeley	N	Y	Berkeley database.
61616	TCP	Apache	N	Y	Message broker.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
22	TCP	SFTP	N	Y	Used to transfer files between SDM servers.

Either port 8080 (HTTP) or port 8443 (HTTPS) must be open on the firewall, depending on which port you select between the network client and SDM server.

> **Note:**
>
> Ports are assigned dynamically through Remote Method Invocation (RMI) dynamic port allocation. If you are enabling and configuring iptables, all traffic must be allowed between servers in the cluster. Communication between clustered SDM servers must not be restricted.

System Support for Encryption and Random Number Generators

The following table describes HTTPS web encryption, password encryption, and safe file transfer system support.

Algorithm(s)	Type	Bit Length	Description
MD5 and SHA-1	Asymmetric	128	Provides the following HTTPS encryption support: • Weak cipher secure socket layer (SSL) Version 2. 0 • Strong cipher SSL 3.0 • Strong Transport Layer Security (TLS) 1.0
OpenBSD-style Blowfish password hashing, described in "A Future-Adaptable Password Scheme" by Niels Provos and David Mazieres.	Symmetric	64	Encrypts stored passwords.
3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, 3des-ctr, arcfour, arcfour128, arcfour256	Asymmetric	128	Provides secure shell version 2 (SSH2) and secure file transfer protocol (SFTP) communications support for file transfer between servers, and between servers to devices.

Web Server Security

During the installation, when you are in the Typical Installation mode, HTTPS is selected for you (by default) as the running mode of your system. We recommend that you maintain the default (HTTPS) to create secure connections over the network. If you have a specific reason for not using the default, you can alternately select HTTP (unsecured). See the *Configure Web*

Server Security section of your Oracle Communications Session Delivery Manager Installation Guide for more information.

> **Note:**
>
> OpenSSL 1.0.1e-fips or later must be installed on your linux server in order to use the HTTPS service on the Apache web server.

HTTPS Certificate Support

Oracle Communications Session Delivery Manager fully supports X.509 certificates and the following certificate extensions are supported through HTTPS:

- .csr—Certificate signing request certificate used in public key infrastructure (PKI) systems.
- .cer—Internet security certificate (CER) in sockets layer (SSL) format that is used by web servers to help verify the identity and security of a site in question. SSL certificates are provided by a third-party security certificate authority such as VeriSign, GlobalSign or Thawte.
- .crt—Certificate is used with a web browser to verify the authenticity of a secure website, and is distributed by certificate authority (CA) companies such as GlobalSign, VeriSign and Thawte. CRT files allow a web browser to connect securely using SSL, and can be viewed by clicking the lock icon within your web browser.
- .der—Distinguished encoding rules certificate provides a method for encoding a data object, such as an X.509 certificate, to be digitally signed or to have its signature verified.

Set the Maximum Upload File Size Limit

You can optionally configure the upload file-size limit, from 2 to 100 gigabytes (GB), for certificate files being uploaded to the web server for its secure operation. See the *Configure Web Server Security* section of your Oracle Communications Session Delivery Manager Installation Guide for more information.

Transport Layer Security Certificates

The transport layer security (TLS) feature provides a single secure sockets layer (SSL) keystore of entity or trusted certificates that provide support for all applications, product plugins, and their respective devices that run on Oracle Communications Session Delivery Manager

- See the *Oracle Communications Session Delivery Manager Installation Guide* for more information about configuring transport layer security certificates.

Secure System Password Guidelines

No default passwords are used in the system, and the system ensures that permissions for generated files (such as temp files, configuration files, and log files) are as restrictive as possible so that they cannot be read or edited. During the system run time, all the passwords obtained, generated, stored, or transmitted are encrypted using password-based encryption (PBE).

Use the following guidelines to create user accounts during the Oracle Communications Session Delivery Manager installation:

1. Use default database accounts that are restricted for access to the local (Oracle) server only. This includes creating an **nncentral** group and **nncentral** user account to set permissions and lock file systems.
2. Create a sudo user account with limited privileges for running the SNMP Trap Relay port (**162**) for Fault Manager.

> **Note:**
>
> The main Oracle Communications Session Delivery Manager process has to run as a sudo user to access port 162.

3. Configure passwords for the **admin** and **LIadmin** user groups before starting Oracle Communications Session Delivery Manager.

Resiliency and High Availability

Oracle Communications Session Delivery Manager offers high availability and resiliency through clustering to create a secure deployment. When the product is deployed in a cluster, it protects the service of multiple individual members if one or more members fail. See your product installation guide for more information.

3

Security Manager Feature Overview

You can use the Oracle Communications Session Delivery Manager Security Manager slider to manage user accounts and maintain the authentication and authorization policies for each user.

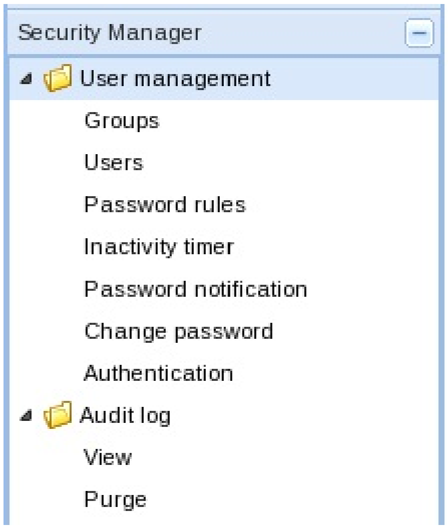
This chapter provides an overview of the Security Manager features. See the *Oracle® Communications Session Delivery Manager Administration Guide* Security Manager chapter for more information about these features and how they are configured.

Security Manager

With administrator privileges, Security Manager allows you to do the following:

- Create and manage users.
- Create and manage groups.
- Configure security authorization levels, policies and privileges for user groups.
- Provide specific access controls for individual user groups, views, and operations.
- Limit access to specific features and functionality for specific users.
- Configure audit log parameters.

Figure 3-1 Security Manager Slider Parameters



User Groups

A user group is a logical collection of users grouped together to access common information or perform similar tasks. You assign specific permissions to a group and then assign users to it. Those users in turn, inherit the group-based permissions.

The following groups are created by default during the installation:

- **None**—Manually configure permissions for this user group.
- **administrators**—This super user group is privileged to perform all operations.
- **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups.
- **provisioners**—This group is privileged to configure Oracle Communications Session Delivery Manager and save and apply the configuration with the exception of a LI configuration.
- **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Session Delivery Manager, and has the fewest privileges.

Users

A user is a person who logs into the system to perform application-related operations. Before this user can access any operations, they must be added to a user group. Each user group has a defined set of privileges. The operations that a user can do depends on the privileges of the user group to which the user belongs.

Operations Tree Structure

The operations tree structure contains all the security configuration and administrative tasks you can perform in SDM. It is logically arranged with parent and child operations that can be accessed once user group and user accounts are created. Individual access to a specific operation within the tree structure can be provided or denied by assigning a privilege to it. Although SDM displays all the operations it supports, some apply only to users who are licensed for a specific application operation.

The top of the operations tree is the root. There can be one or more operation categories below the root that serve as parents for individual operations (children). The child privilege type of higher-level (or parent) operation is equal or less than the privilege type of its parent. When you change the privilege type of a parent, the child privilege type can change based on this rule. However, if the parent privilege type is returned to its previous privilege type, the child remains at the privilege type to which it was bumped and needs to be promoted manually.

Apply or Change User Group Privileges

You can apply privileges to user groups that you add to allow or deny all users within this user group the ability to perform certain operations. This includes items intended for use with separate application products. For the default **LIAdministrators**, **administrators**, **provisioners**, and **monitor** user groups, only device group privileges can be changed.

Note:

All user group privileges that are available through SDM are described in the following sections. You may not see some of these user group privileges in the **Configuration**, **Device maintenance**, **Administrative operations**, **Fault management**, **Device groups**, and **Applications** tabs in SDM until you install your product plugin.

Set the User Inactivity Timer to Prevent Unauthorized Access

We recommend configuring the inactivity timer to prevent unauthorized access to the system.

The inactivity timer logs off the user from the Oracle Communications Session Delivery Manager session when its value is exceeded. The user must re-enter their password to continue. You can set different values for a user with administrative permissions and users who do not have administrative permissions.

Audit Logs

You can use the audit log (containing audit trails) generated by SDM to view performed operations information, which includes the time these operations were performed, whether they were successful, and who performed them when they were logged into the system.

Note:

Audit logs contain different information depending on its implementation.

Audit trails include the following information:

- The user who performed the operation.
- What operation was performed by the user.
- When the operation was performed by the user.
- Whether the operation performed by the user was successful or failed.

Configure External User Authentication

Users who belong to the external domain user group are authenticated outside of SDM by an external domain server. You can select either a RADIUS domain server or Active Directory (AD) domain controller:

- A RADIUS server provides centralized Authentication, Authorization, and Auditing/ Accounting (AAA) security protocol management for users who connect and use a network service.
- An AD domain controller provides a directory service in a Windows domain type network using Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

An external domain user group must be mapped to an internal (local) user group in SDM so that this external domain user group and its users inherit the authorization privileges that are specific to the local user group.

Note:

Internal and external users are both supported simultaneously. However, external users do not have corresponding stored user records or username and password information.

4 Security Maintenance

Use the security maintenance practices in this chapter to keep Oracle Communications Session Delivery Manager secure.

Security Checklist

Use the following checklist to secure Oracle Communications Session Delivery Manager before, during and after its installation.

1. Do **NOT** connect your system to any untrusted networks, especially the Internet, until all protections have been configured. Customers have reported systems under configuration compromised within minutes due to incomplete configurations.
2. If you use identity management or single sign-on (SS) technologies, ensure that they are supported by security assertion markup language (SAML).
3. Harden the management environment.
   a. Make sure all equipment is in locked cabinets or at least in a secure room.
   b. Set strong passwords for all accounts and system users (nncentral user and nncentral group, sudo user, e-mail user, the admin user, LIadmin user etc.) during the installation.
   c. During the system installation, use **HTTPS** (default) as the system running mode.
   d. Use secure protocols, such as SFTP, HTTPS, LDAP and SSH, to communicate with Oracle Communications Session Delivery Manager.
4. Once Oracle Communications Session Delivery Manager is started, use the Security Manager to limit user privileges:
   a. Carefully consider who has access to the **administrators** password.
   b. Authenticate local groups and users that access the system. The system comes with the following default user groups: **monitor**, **provisioner**, **administrators**, and **LIadministrators.** Administrators have a complete set of permissions only, and the system provides role-based security policies for access control with dedicated user accounts that have pre-assigned privilege levels.
   c. Authenticate and authorize external users through an existing RADIUS server or Active Directory (AD) server.
5. Configure the inactivity timer in Security Manager to stop the abuse of system services.
6. Use HP Fortify, HP WebInspect, and Tenable Nessus scans to perform static and dynamic security testing on Oracle Communications Session Delivery Manager periodically, or after each release.
7. Continue to monitor system activity to determine if someone is attempting to abuse system services and to detect if there is performance or availability problems. Useful monitoring information can be acquired through audit logs, system logs and SNMP.

Maintain Security Updates

You must install all security patch releases for Oracle Communications Session Delivery Manager software when they appear or as soon as possible to keep your system secure.

Oracle constantly reviews the latest security vulnerabilities, applies any required critical security patch (including any third-party components) to the Oracle Communications Session Delivery Manager software, and issues a security patch release with release notes that describe these updates. See the Critical Patch Updates and Security Alerts web page for these updates and other current security information. You can also use the instructions on this web page to receive email notifications for the following announcements:

- Critical Patch Updates
- Security Alerts
- Third Party Bulletins
- Fixed Public Vulnerabilities
- Policies
- Security Vulnerability Reports

Security Considerations for Developers

We highly recommended that application developers fully secure the link between the Web services application (Web service client) and follow secured coding standards.

Oracle Communications Session Delivery Manager offers a REST Application Programming Interface (API) and a SOAP/XML provisioning API to allow users to write applications that automate the provisioning of network elements. See the *REST API for Oracle® Communications Session Delivery Manager Release 8.0* for more information.

> **Note:**
>
> The *Oracle® Communications Session Element Manager SOAP/XML Provisioning API Guide, Release 8.0* is deprecated.

You can use these APIs to perform operations against network elements managed by an Oracle Communications Session Delivery Manager server, and data structures used as input and output parameters for those operations. These operations are invoked by a client application to provision network elements.

Database Redundancy

Use backup and restore scripts to implement the database geographic (GEO) redundancy. See the *Oracle® Communications Session Delivery Manager Administration Guide, Release 8.0* for more information.