Oracle® Communications LSMS Query Server

Security Guide

Release 13.2

E76244 Revision 1

July 2016

Oracle Communications LSMS Query Server Security Guide, Release 13.2

Copyright © 2003, 2016, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Table of Contents

List of Tables

Chapter 1

Introduction

Topics:

This chapter contains general information such as an overview of the manual, how to get technical assistance, and where to find additional information.

Overview

This manual describes how to ensure a secure installation of Oracle Communications LSMS (LSMS) Query Server, and explains LSMS Query Server security features.

Scope and Audience

This manual is intended for system administrators that are installing and configuring an LSMS Query Server.

Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

Icon	Description
DANGER	Danger: (This icon and text indicate the possibility of *personal injury*.)
WARNING	Warning: (This icon and text indicate the possibility of *equipment damage*.)
CAUTION	Caution: (This icon and text indicate the possibility of *service interruption*.)
TOPPLE	Topple: (This icon and text indicate the possibility of *personal injury* and *equipment damage*.)

Manual Organization

This manual contains the following chapters:

- *Introduction* contains general information such as an overview of the manual, how to get technical assistance, and where to find more information.
- *LSMS Query Server Security Overview* describes basic security considerations and provides an overview of LSMS Query Server security.
- *Performing a Secure LSMS Query Server Installation* describes the process to ensure a secure installation of LSMS Query Server.
- *Implementing LSMS Query Server Security* explains LSMS Query Server security features.
- *Security Considerations for Developers* provides guidelines for developers.

My Oracle Support (MOS)

MOS (*https://support.oracle.com*) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with MOS registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select **2** for New Service Request
2. Select **3** for Hardware, Networking and Solaris Operating System Support
3. Select one of the following options:
   - For Technical issues such as creating a new Service Request (SR), Select **1**
   - For Non-technical issues such as registration or assistance with MOS, Select **2**

You will be connected to a live agent who can assist you with MOS registration and opening a support ticket.

MOS is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or by calling the Oracle Support hotline for your local country from the list at *http://www.oracle.com/us/support/contact/index.html*. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system’s ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations

- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Related Specifications

For information about additional publications that are related to this document, refer to the Oracle Help Center site. See *Locate Product Documentation on the Oracle Help Center Site* for more information on related product publications.

Customer Training

Oracle University offers training for service providers and enterprises. Visit our web site to view, and register for, Oracle Communications training:

http://education.oracle.com/communication

To obtain contact phone numbers for countries or regions, visit the Oracle University Education web site:

www.oracle.com/education/contacts

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, *http://docs.oracle.com*. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at *http://www.adobe.com*.

1. Access the Oracle Help Center site at *http://docs.oracle.com*.
2. Click **Industries**.
3. Under the Oracle Communications subheading, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets will appear under the headings “Network Session Delivery and Control Infrastructure” or “Platforms.”
4. Click on your Product and then the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Chapter 2

LSMS Query Server Security Overview

Topics:

This chapter describes basic security considerations and provides an overview of LSMS Query Server security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols using TLS (SSL), and secure passwords. See *Performing a Secure LSMS Query Server Installation* for more information.
- **Learn about and use the LSMS Query Server security features.** See *Implementing LSMS Query Server Security* for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See *Security Considerations for Developers* for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site: *http://www.oracle.com/technetwork/topics/security/alerts-086861.html*

When planning your LSMS Query Server implementation, consider the following questions:

- Which resources need to be protected?
  - You need to protect customer data, such as telephone number (TN) information and associated data.
  - You need to protect internal data, such as proprietary source code.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- Who are you protecting data from?

  For example, you need to protect your subscribers' data from other subscribers, but someone in your organization might need to access that data to manage it. You can analyze your work flows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- What happens if protections on strategic resources fail?

  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Overview of LSMS Query Server Security

The optional LSMS Query Server enables automatic access to real time Local Number Portability (LNP) data through a standard API. Customers can perform customized, high volume, automated data queries for use by internal office and support systems such as service assurance, testing, service fulfillment, and customer care.

Operating System Security

An LSMS Query Server is hosted by a dedicated Oracle SPARC server running the Oracle Solaris 10/11 operating system. Solaris handles all operating system security for the LSMS Query Server, and the LSMS Query Server *Installation and Upgrade Guide* assumes that servers already have SPARC Solaris 10/11 installed. Make sure you always have the latest SPARC Solaris software/patches installed on your machines.

Database Security

The following security considerations apply to the MySQL database:

- Secure Database Access Credentials

  Only authorized personnel are allowed to access the database and a user ID and password are required.

  Provide minimum privileges to the user so that unauthorized modifications can be avoided.

  For more information, see *Managing User Accounts*.

- Use IPsec Connections for Data Downloads

  Configure an IPsec connection to download data to customer servers or devices.

  IP Security (IPsec) secures Internet Protocol (IP) communications by encrypting and/or authenticating all IP packets. IPsec provides security at the network layer for connections configured for specified addresses.

- Use SSH/SSL Connections

  SSH/SSL is a robust, commercial-grade, and full-featured toolkit that implements the security and network encryption. SSH/SSL provides secure data transmission through encryption keys.

  Encryption is strongly recommended for any remote connection to an LSMS Query Server. For more information about using keys, refer to the *Configuration Guide*.

Chapter 3

Performing a Secure LSMS Query Server Installation

Topics:

This chapter describes the process to ensure a secure installation of LSMS Query Server.

For step-by-step instructions to install an LSMS Query Server, refer to the LSMS Query Server *Installation and Upgrade Guide*.

Pre-Installation Configuration

All pre-installation configuration is set by Solaris 10/11. No additional user configuration regarding security is required.

Installing LSMS Query Server Securely

The Oracle Solaris 10/11 operating system running on an Oracle SPARC server ensures a secure installation of the LSMS Query Server application. For step-by-step instructions to install the LSMS Query Server, refer to the LSMS Query Server *Installation and Upgrade Guide*. The installation procedure assumes that servers already have SPARC Solaris 10/11 installed. Make sure you always have the latest SPARC Solaris software/patches installed on your machines.

Post-Installation Configuration

There are no required post-installation configuration changes pertaining to Security.

For general information about configuring the Query Server, refer to the *Configuration Guide*.

Chapter 4

Implementing LSMS Query Server Security

Topics:

This chapter explains the LSMS Query Server security features.

Managing User Accounts

The system administrator assigns user names and passwords.

Other than the platform-installed users, the only application and therefore the only users for the LSMS Query Server are MySQL users.

The MySQL admin user should limit additional users to only those privileges required. Refer to the Oracle *MySQL Reference Manual* for further details.

Configurable MySQL Port

The master port configuration on the LSMS Query Server must match the port configured in the LSMS GUI for the corresponding, mated LSMS pair. For information about setting the master port on the Query Server, refer to the LSMS Query Server *Installation and Upgrade Guide*.

The optional Configurable MySQL Port feature enhances the security of LSMS Query Server databases by enabling the system administrator to change the MySQL port. The port can be changed in the `my.cnf` file and the same port should be set for the corresponding Query Server IP address through the LSMS GUI. The MySQL port can be configured to ports 1024-65535.

Chapter 5

Security Considerations for Developers

This chapter provides information for developers about how to create secure applications for LSMS Query Server, and how to extend LSMS Query Server without compromising security.

Consider the following guidelines:

- Use encrypted (hashed) passwords for user-accessible files.
- Delete or disable unused user accounts.
- Remove redundant code.

Glossary

A

API

Application Programming Interface

An interface with commands, possibly routines and/or macros, provided by an operating system or an add-on for an operating system (that support network use, for example). Application programs can use this interface to tell the operating system to perform specific actions.

I

IPsec

Internet Protocol Security

A protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a data stream.

L

LNP

Local Number Portability

The ability of subscribers to switch local or wireless carriers and still retain the same phone number.

LSMS

Local Service Management System

An interface between the Number Portability Administration Center (NPAC) and the LNP service databases. The LSMS receives LNP data from the NPAC and downloads that data to the service databases. LNP data can be entered into the LSMS database. The data can then be downloaded to the LNP service databases and to the NPAC.

S

SSH

Secure Shell

A protocol for secure remote login and other network services over an insecure network. SSH encrypts and authenticates all EAGLE IPUI and MCP traffic, incoming and outgoing (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks.

SSL

Secure Socket Layer (SSL) is an industry standard protocol for clients needing to establish secure (TCP-based) SSL-enabled network connections