Oracle® Communications Charging Traffic Monitor

Security Guide

Release 12.1

E80471-01

March 2017

Oracle Communications Charging Traffic Monitor Security Guide, Release 12.1

E80471-01

Contents

Preface

This document provides guidelines and recommendations for setting up Oracle Communications Charging Traffic Monitor in a secure configuration.

Audience

This guide is intended for systems administrators, database administrators, network administrators, and operations personnel who install and administer Charging Traffic Monitor.

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 more information about Charging Traffic Monitor security, see the following documents in the Charging Traffic Monitor documentation set:

- *Oracle Communications Charging Traffic Monitor Installation and System Administration Guide*

To implement security, Charging Traffic Monitor also uses other Oracle products, such as Oracle Database and Oracle WebLogic Server. See the following documents for more information about securing those products:

- *Oracle Database Security Guide*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*

Oracle documentation is available from Oracle Help Center:

`http://docs.oracle.com`

Document Revision History

The following table lists the revision history for this document:

Version	Date	Description
E80471-01	March 2017	Initial release.

1

Charging Traffic Monitor Overview

This chapter provides an overview of Oracle Communications Charging Traffic Monitor security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** Update software to the latest product release and apply patches, if available.
- **Limit privileges as much as possible.** Only give users access that is 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, how often, and monitor those components.
- **Install software securely.** Use firewalls, secure protocols (such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL)), and secure passwords. See "Performing a Secure Charging Traffic Monitor Installation" for more information.
- **Learn about and use the Charging Traffic Monitor security features.** See "Performing a Secure Charging Traffic Monitor Installation" for more information.
- **Keep up to date on security information.** Install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" website:

  `https://www.oracle.com/technetwork/topics/security/alerts-086861.html`

  Oracle regularly issues security-related patch updates and security alerts.

Overview of Charging Traffic Monitor Security

Charging Traffic Monitor comprises various components, and each performs its own security-level functions. The key components and their security related functions are:

- **Oracle WebLogic Server** provides end user applications deployed on WebLogic Server with secured access based on user roles and credentials, and it provides user management capabilities. You can enable secure sockets layer (SSL) for Charging Traffic Monitor on outward-facing ports by enabling encryption through WebLogic Server. User access to WebLogic Server is available through the SSL encryption.

Note: WebLogic Server certificates must be replaced with your own SSL certificates after deployment.

- **Oracle Database Server** stores Charging Traffic Monitor-generated statistical data, which is accessed through secured credentials. Credentials are encrypted using Oracle wallet. Oracle Database provides user management capabilities.

Understanding the Charging Traffic Monitor Environment

When planning Charging Traffic Monitor implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data, such as the subscriber ID that includes the International Mobile Subscriber Identity (IMSI), the Mobile Station ISDN Number (MSISDN), the International Mobile Equipment (IMEI), and the Network Access Identifier (NAI).
  - 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 must 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 workflows to determine who needs access to the data; for example, a system administrator can manage your system components without needing to access the system data.
- **What will happen 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.

Recommended Deployment Configurations

This section describes default settings and security features used by Charging Traffic Monitor. Then it describes recommended deployment configurations for used components.

There is a standard deployment model and provisioning for Charging Traffic Monitor. The workflow for said deployment can be found in "Performing a Secure Charging Traffic Monitor Installation." Deploying Charging Traffic Monitor requires the following components:

- Oracle Database.
- Oracle WebLogic Server.

The Charging Traffic Monitor processing engine connects to Oracle Database and facilitates data movement, such as reports and key performance indicators (KPIs). Users can access the Charging Traffic Monitor user interface through WebLogic Server, which displays the data stored in Oracle Database. To ensure secure data transfer, deploy and co-locate these components in a secured network over a local area network (LAN). Managing security for data movement across a LAN ensures that all of the components operate behind a firewall, allowing only secured user access to the applications.

Each of the components has its own secure installation features. However, instances exist where data movement occurs from one component to another.

Charging Traffic Monitor Security

Charging Traffic Monitor security involves the following:

- Operating System Security
- Oracle Database Security
- Oracle WebLogic Server Security

Operating System Security

Charging Traffic Monitor does not require specific operating system security configurations other than firewall configuration. Table 1–1 lists the Charging Traffic Monitor ports and protocols:

Table 1–1 Charging Traffic Monitor Ports and Protocols

Protocol	Port	Inbound	Outbound	Description
JDBC	1521	Database	Weblogic Server	Database access
HTTP	4040	Spark Streaming	-	-
SSL	9093	Kafka	Kafka broker	Data transfer from the vCollector probe to the KPI engine.
SSL	7001/7002	WebLogic Server	-	-

In addition, the Charging Traffic Monitor installation is run with root privileges. For more information, see "Installing Charging Traffic Monitor on the Server Hosting Oracle Database and WebLogic Server".

For more information about operating system security, see the following documents:

- *Oracle Linux - Security Guide for Release 7*
- *Tips for Hardening on Oracle Linux Server*

> **Note:** Oracle recommends that you avoid using a NFS shared location or using minimum restrictions for data ingestion.

Oracle Database Security

Charging Traffic Monitor does not require specific security configurations for Oracle Database. During the Charging Traffic Monitor installation, Charging Traffic Monitor database users are created and their access credentials are added into a Oracle wallet, which is saved in a restricted access folder.

For more information about securing Oracle Database, see the following documents:

- *Oracle Database Security Guide*
- *Oracle Database Advanced Security Administrator's Guide*

Note: Oracle recommends activating data with REST encryption if sensitive data is stored in Oracle database, such as in the Charging Traffic Monitor schema.

Charging Traffic Monitor does not use any default passwords. Passwords are prompted during the Charging Traffic Monitor post-installation configuration process.

Oracle WebLogic Server Security

Charging Traffic Monitor does not require specific security configurations for WebLogic Server.

Note: HTTPS configuration and password access is recommended to protect exchanged data.

For information about securing WebLogic Server, see *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

2

Performing a Secure Charging Traffic Monitor Installation

This chapter describes recommended installation steps and explains how to securely install and configure Oracle Communications Charging Traffic Monitor.

For more information about installing Charging Traffic Monitor, see *Oracle Communications Charging Traffic Monitor Installation and System Administration Guide.*

Pre-Installation Tasks

Install and configure the following components before installing Charging Traffic Monitor:

- Oracle Database.
- Oracle WebLogic Server.

When you run the Charging Traffic Monitor Red Hat Package Manager (RPM), you will need to know the credentials for several users, for example the Oracle Database and WebLogic Server administrators. For more information, see *Oracle Communications Charging Traffic Monitor Installation and System Administration Guide*.

Installing Charging Traffic Monitor

This section provides a workflow overview of a typical Charging Traffic Monitor installation:

1. Install Charging Traffic Monitor engine on the server on which Oracle Database and WebLogic Server are installed.
2. Install the vCollector probe on a server that has secure socket shell (SSH) access.
3. Update the **ctm-configuration-param** configuration file with the required values, including user credentials. If a value is not provided the user is prompted to enter a value during the Charging Traffic Monitor post-installation task.

Installing Charging Traffic Monitor on the Server Hosting Oracle Database and WebLogic Server

Run the Charging Traffic Monitor RPM as the **root** user.

Users and Schemas

The Charging Traffic Monitor RPM creates a Charging Traffic Monitor schema.

All parameters except passwords are stored in the Oracle wallet.

Wallet File

The installer creates an Oracle wallet file containing access information to the different Charging Traffic Monitor components and schema in a dedicated secured folder. The **ctm-configuration-param** configuration file contains the access credentials.

> **Note:** Outside of this Oracle wallet file, none of the credential information is stored in any Charging Traffic Monitor file or database.

WebLogic Server

The installation process creates a new WebLogic Server instance dedicated to Charging Traffic Monitor. The installer will prompt the user for the WebLogic Server **admin** user credentials if not provided in the **ctm-configuration-param** configuration file.

In the Charging Traffic Monitor instance, a realm is created with default roles. Charging Traffic Monitor also configures data source access (Oracle Database) through the Oracle wallet file. Hence, the Oracle wallet file generated on Oracle Database is synchronized on the Application server through the common installer.

Installing the vCollector Probe on a Server with SSH Access

Run the vCollector probe RPM as the **root** user.

Users

The vCollector probe RPM creates the **ctmusr** user and the **ctmgrp** group.

All the vCollector probe parameters are stored in the **rat.conf** file. A secure sockets layer (SSL) certificate is required to connect to the Kafka broker with a SSL connection.

Post-Installation Tasks

This section explains the post-installation configurations that are completed after Charging Traffic Monitor is installed. To perform these tasks, you need the credentials for several users, for example the Charging Traffic Monitor administrative user and the operating system user. For more information, see *Oracle Communications Charging Traffic Monitor Installation and System Administration Guide*.

Configuring Charging Traffic Monitor Securely

There are several configurations that need to be completed to secure Charging Traffic Monitor.

SSH Connection for Ingestion

The vCollector probe pulls data from the online charging system (OCS) by either a Network switch with port mirroring or a Network Tap.

Secure socket shell (SSH) must be enabled on the server that will host the vCollector probe.

Oracle Wallet Management

Communication authentication to and from Oracle Database are created in the Oracle wallet. The Oracle wallet is automatically generated or updated on the Charging

Traffic Monitor host by the Charging Traffic Monitor install scripts. When access credentials change the Oracle wallet must be updated. For a discussion on how to update the Oracle wallet, see the Oracle Database documentation.

Post-Installation on Application Server

The Charging Traffic Monitor administrator manages the WebLogic Server realm to create a new user and assign users to roles defined by Charging Traffic Monitor.

The Charging Traffic Monitor RPM creates a **ctmusr** user and **ctmgrp** group.

Changing Default Passwords

Follow the standard database procedures to change the Charging Traffic Monitor account and credential information.

> **Note:** If you change account and credential information, regenerate and re-synchronize the Oracle wallet on all servers.

Use the WebLogic Server console to change WebLogic Server credentials. For more information, see the Oracle WebLogic Server documentation.

A

Charging Traffic Monitor Secure Deployment Checklist

This appendix provides security guidelines for Oracle Communications Charging Traffic Monitor.

Security Guidelines

The following security checklist provides guidelines to help you secure Charging Traffic Monitor and its components.

- Install only what is required.
- Don't install any third party components into the operating system account that is used for installing the product.
- Lock and expire default user accounts.
- Enforce password management.
- Practice the principle of least privilege.
  - Grant only the necessary privileges.
    - Revoke unnecessary privileges from the PUBLIC user group.
    - Restrict permissions on run-time facilities.
- Enforce access controls effectively, and authenticate clients stringently.
- Restrict network access:
  - Use a firewall.
  - Never poke a hole through a firewall.
  - Monitor who accesses your systems.
  - Check network IP addresses.
- Apply all security patches and work arounds.
- Contact Oracle Security Products if you come across a vulnerability in Oracle Database or WebLogic Server.