Oracle® Configuration Manager

Security Overview

Release 10.3.7

E27244-01

March 2012

When installing any new software onto a machine, there is always a concern that corporate security may be compromised. This document explains how Oracle Configuration Manager addresses these concerns.

Introduction

Oracle Configuration Manager (OCM) collects configuration information and, if running in connected mode, automatically uploads it to an Oracle repository. When the configuration data is uploaded on a regular basis, support analysts can analyze this data and provide better support and assistance.

Oracle Configuration Manager benefits your organization by:

- Reducing time for resolution of support issues
- Providing pro-active problem avoidance
- Improving access to best practices and the Oracle knowledge base
- Improving understanding of your business needs
- Providing consistent responses and services

> **Note:** OCM does not collect business transactions, production data, or passwords.

Much of the configuration information collected by OCM may be collected by other means when there is a support issue. OCM simplifies this data collection, improves the accuracy and reliability of the information and provides secure transmission of the data back to Oracle.

Oracle security teams carefully review all proposed enhancements to OCM to ensure that all data collected is used only to facilitate more efficient use of Oracle products and services, including Oracle Support.

Communications Between the Customer Site and Oracle

When transmitting data between your site and Oracle, a key security concern is to ensure that only Oracle accesses the data. To protect against unauthorized access, Oracle uses Secure Socket Layer (SSL) and HTTPS for all communications.

When transmitting data, the first step authenticates Oracle as the recipient by interrogating the certificate returned by the server. A recognized certificate authority, specified by Oracle, issues the certificate to Oracle Corporation.

Once authentication is complete, OCM requires that 128-bit encryption using public/private key exchange (otherwise known as asymmetric encryption) be used for all communications. OCM initiates outbound communications with Oracle and does not listen for inbound communications, so that your firewall protections are preserved.

If you are unable to establish an HTTPS connection from your environment, OCM can be configured to run in disconnected mode. While running in disconnected mode, OCM will not collect data automatically nor attempt to connect to Oracle; performing a configuration collection produces an output file that can then be manually uploaded to Oracle by way of My Oracle Support.

Viewing Collected Data

OCM permits your users to view and verify the configuration data that is collected and transmitted to Oracle. The output of configuration collections is stored on the local host for viewing; those XML files are the ones uploaded to Oracle. These XML files may be found in the OCM_INSTALL_ROOT/ccr/host/<hostname>/state/review directory.

Oracle also makes available a document, called ocm_collections.pdf, containing all of the configuration parameters that OCM is capable of collecting (any individual collection will contain a subset of these configuration items). This document can be found in the OCM_INSTALL_ROOT/doc directory.

Customer Configuration Repository

The customer configuration repository (CCR) is secured inside the Oracle data center and protected by Oracle network security infrastructure and security teams. All access to the CCR goes through a rigorous security review.

Collecting Database Information

Traditionally, data is collected from a database by making a connection to the database and passing user credentials. The disadvantages of this approach are that credentials have to be stored and password changes have to be tracked over time.

OCM has implemented a different approach:

1. OCM instructs the database to collect its own configuration and write that configuration to a report or file within the $ORACLE_HOME/ccr/state directory. Only the owner of Oracle Home can read the contents of the configuration report generated.
2. During the installation of OCM, the installCCRSQL.sh script creates an account in the database to house a PL/SQL procedure, installs a PL/SQL package and sets up a DBMS job so that the procedure is executed on a regular basis.

   To avoid security vulnerabilities, the account that OCM creates is immediately locked and the password expired. This can be done because OCM does not connect to the database for collections. The account is only needed to house the PL/SQL procedure.

Auto-Update Capability

Auto-update provides the ability to automatically detect, authenticate and apply the latest package updates to OCM. This allows you to maintain the OCM software without the need to apply patches or upgrade software or configuration over time. By default, auto-update capability is enabled when you install and configure OCM.

As with any interaction with Oracle Support, the communication link is authenticated and encrypted. Once the server is authenticated, any OCM package updates, which are digitally signed by Oracle, are downloaded to a staging directory. Before an update is applied to the OCM installation, the digital signature is validated. This process confirms that the update was signed with a certificate issued to Oracle by a specific certificate authority. This certificate is different from the certificate used to secure the communications link. The update is applied to the OCM installation only if this entire process passes validation.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.
