Oracle® Configuration Manager

Security Overview

Release 10.3.0

E12881-01

August 2008

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 via MetaLink.

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/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

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, 7 days a week. For TTY support, call 800.446.2398. Outside the United States, call +1.407.458.2479.

Oracle Configuration Manager Security Overview, Release 10.3.0
E12881-01

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.