Oracle® Retail Predictive Application Server and Applications Cloud Edition

Security Guide

Release 17.0

E92944-01

January 2018

Oracle Retatil Predictive Application Server and Applications Cloud Edition Security Guide, Release 17.0

E92944-01

Copyright © 2018, Oracle and/or its affiliates. All rights reserved.

Primary Author: Judith Meskill

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.

Value-Added Reseller (VAR) Language

Oracle Retail VAR Applications

The following restrictions and provisions only apply to the programs referred to in this section and licensed to you. You acknowledge that the programs may contain third party software (VAR applications) licensed to Oracle. Depending upon your product and its version number, the VAR applications may include:

(i) the **MicroStrategy** Components developed and licensed by MicroStrategy Services Corporation (MicroStrategy) of McLean, Virginia to Oracle and imbedded in the MicroStrategy for Oracle Retail Data Warehouse and MicroStrategy for Oracle Retail Planning & Optimization applications.

(ii) the **Wavelink** component developed and licensed by Wavelink Corporation (Wavelink) of Kirkland, Washington, to Oracle and imbedded in Oracle Retail Mobile Store Inventory Management.

(iii) the software component known as **Access Via**™ licensed by Access Via of Seattle, Washington, and imbedded in Oracle Retail Signs and Oracle Retail Labels and Tags.

(iv) the software component known as **Adobe Flex**™ licensed by Adobe Systems Incorporated of San Jose, California, and imbedded in Oracle Retail Promotion Planning & Optimization application.

You acknowledge and confirm that Oracle grants you use of only the object code of the VAR Applications. Oracle will not deliver source code to the VAR Applications to you. Notwithstanding any other term or condition of the agreement and this ordering document, you shall not cause or permit alteration of any VAR Applications. For purposes of this section, "alteration" refers to all alterations, translations, upgrades, enhancements, customizations or modifications of all or any portion of the VAR Applications including all reconfigurations, reassembly or reverse assembly, re-engineering or reverse engineering and recompilations or reverse compilations of the VAR Applications or any derivatives of the VAR Applications. You acknowledge that it shall be a breach of the agreement to utilize the relationship, and/or confidential information of the VAR Applications for purposes of competitive discovery.

The VAR Applications contain trade secrets of Oracle and Oracle's licensors and Customer shall not attempt, cause, or permit the alteration, decompilation, reverse engineering, disassembly or other reduction of the VAR Applications to a human perceivable form. Oracle reserves the right to replace, with functional equivalent software, any of the VAR Applications in future releases of the applicable program.

Contents

Send Us Your Comments

Oracle Retail Predictive Application Server and Applications Cloud Edition Security Guide, Release 17.0

Oracle welcomes customers' comments and suggestions on the quality and usefulness of this document.

Your feedback is important, and helps us to best meet your needs as a user of our products. For example:

- Are the implementation steps correct and complete?
- Did you understand the context of the procedures?
- Did you find any errors in the information?
- Does the structure of the information help you with your tasks?
- Do you need different information or graphics? If so, where, and in what format?
- Are the examples correct? Do you need more examples?

If you find any errors or have any other suggestions for improvement, then please tell us your name, the name of the company who has licensed our products, the title and part number of the documentation and the chapter, section, and page number (if available).

Note: Before sending us your comments, you might like to check that you have the latest version of the document and if any concerns are already addressed. To do this, access the Online Documentation available on the Oracle Technology Network Web site. It contains the most current Documentation Library plus all documents revised or released recently.

Send your comments to us using the electronic mail address: retail-doc_us@oracle.com

Please give your name, address, electronic mail address, and telephone number (optional).

If you need assistance with Oracle software, then please contact your support representative or Oracle Support Services.

If you require training or instruction in using Oracle software, then please contact your Oracle local office and inquire about our Oracle University offerings. A list of Oracle offices is available on our Web site at http://www.oracle.com.

Preface

This document serves as a guide for administrators, developers, and system integrators who securely administer RPASCE and RPASCE applications. Installation and configuration for each product are covered in more detail in the each product's Installation Guide.

Audience

This document is intended to provide an overview of the security features of the RPASCE Platform and applications built upon it. It contains a set of best practices for administrators, developers, and system integrators who perform the following functions:

- Work with customers to configure and deploy RPASCE applications.
- Perform RPASCE Administration tasks such as user management, permissions, and system limits.

This document is not intended to describe in detail the processes of deploying and maintaining an RPASCE application. It is assumed that the readers have a general knowledge of administering the underlying technologies and applications.

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

This document serves as a guide for administrators, developers, and system integrators who securely administer, customize, and integrate Oracle Retail Predictive Application Server Cloud Edition and RPASCE applications. Information on securing the following RPASCE applications is included in this guide:

For more information, see the following documents in the RPASCE documentation set:

- Oracle Retail Item Planning Cloud Service
- Oracle Retail Merchandise Financial Planning Cloud Service
- Oracle Retail Merchandise Financial Planning Enterprise Edition Cloud Service

Customer Support

To contact Oracle Customer Support, access My Oracle Support at the following URL:

`https://support.oracle.com`

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received
- Screen shots of each step you take

Improved Process for Oracle Retail Documentation Corrections

To more quickly address critical corrections to Oracle Retail documentation content, Oracle Retail documentation may be republished whenever a critical correction is needed. For critical corrections, the republication of an Oracle Retail document may at times not be attached to a numbered software release; instead, the Oracle Retail document will simply be replaced on the Oracle Technology Network Web site, or, in the case of Data Models, to the applicable My Oracle Support Documentation container where they reside.

This process will prevent delays in making critical corrections available to customers. For the customer, it means that before you begin installation, you must verify that you have the most recent version of the Oracle Retail documentation set. Oracle Retail documentation is available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

An updated version of the applicable Oracle Retail document is indicated by Oracle part number, as well as print date (month and year). An updated version uses the same part number, with a higher-numbered suffix. For example, part number E123456-02 is an updated version of a document with part number E123456-01.

If a more recent version of a document is available, that version supersedes all previous versions.

Oracle Retail Documentation on the Oracle Technology Network

Oracle Retail product documentation is available on the following web site:

`http://www.oracle.com/technetwork/documentation/oracle-retail-100266.html`

(Data Model documents are not available through Oracle Technology Network. You can obtain them through My Oracle Support.)

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Overview

The Oracle Retail Predictive Application Server Cloud Edition (RPASCE) is a platform that provides a set of common components used by a number of applications (or solutions). For these solutions, RPASCE provides the infrastructure needed to store, process, and produce information based on data input by the retailer.

This guide discusses security considerations around end user maintenance of an RPASCE Server application and the users of an RPASCE application.

Terminology

The following section provides a brief introduction to RPASCE and its terminology.

RPASCE Concepts

- **RPASCE**: A platform that provides a foundation to run solutions used for retail planning. RPASCE provides those solutions with a common interface based on wizards, templates, workbooks, and batch processes.
- **RPASCE Solution**: An application running on top of RPASCE that provides solutions for retail problems such financial planning or forecasting demand.
- **RPASCE Domain**: A collection of server side directories and files containing the data and procedures required to execute a specific RPASCE solution. Domains may be:
  - **Global**: contains data above the partition level as well as settings and metadata that apply across all local domains
  - **Local**: contains data for a single partition (for example, for one department in the product hierarchy)

Note: RPASCE users who are given access to only certain partitions may only have access to a subset of local domains. All users have access to the global domain.

RPASCE Applications

Users access an RPASCE solution through the RPASCE client, a web-based client.

In addition, Administrators can access the **Configuration Tools**. This is a Windows based set of utilities used to configure and maintain a RPASCE Solution.

Security Guides

As well as the RPASCE Security Guide, Security Guides exist for other applications such as the WebLogic server. Information on these is available on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation`

RPASCE Client

Users connect to RPASCE applications using the RPASCE Client. The RPASCE Client is a web-based application that allows access to RPASCE workbooks through interaction with the web server in users' browsers.

Dependent Applications

Security guides are available for the following dependent applications:

- Oracle Access Manager
- Oracle HTTP Server
- Oracle Internet Directory
- Oracle WebLogic

These Security Guides may be found on the Oracle Technology Network at the following URL:

`http://www.oracle.com/technetwork/documentation`

General Security Principles

The following principles are fundamental to using any application securely.

Keep Software Up to Date

One of the principles of good security practice is to keep all software versions and patches up to date. Since all interactions with RPASCE Applications happen through the web browser and the FTP client, these should be maintained at their latest release level for all client systems.

Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. Over ambitious granting of responsibilities, roles, grants, and so on, especially early on in an organization's life cycle when people are few and work needs to be done quickly, often leaves a system wide open for abuse. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

Monitor System Activity

System security stands on three legs: good security protocols, proper system configuration and system monitoring. Auditing and reviewing audit records address this third requirement. Each component within a system has some degree of monitoring capability. Follow audit advice in this document and regularly monitor audit records.

Keep Up to Date on Latest Security Information

Oracle continually improves its software and documentation. Check this note yearly for revisions.

2

Client Tier Security

This chapter discusses security for the RPASCE Client.

Factors Affecting Security

The factors affecting security are Authentication, Authorization, and Auditing.

Authentication

RPASCE Client uses an external authentication model that uses pluggable plugged-in authentication providers in the WebLogic Server.

RPASCE Client has been certified for Single Sign-On (SSO) authentication using Oracle SSO. Other third-party providers, while conforming to the SSO authentication architecture, are not certified for use with the RPASCE Client.

Users and user groups that are set up in the Oracle Internet Directory (OID) are authorized to access the RPASCE Client during the installation process. The installation properties input.security.group and input.security.user are used to specify a comma-separated list of user names and group names, respectively.

Only user groups must be specified during installation. The property input.security.user can be left empty. This approach facilitates the easy addition or removal of users by the addition or deletion of users from the authorized groups.

After installation, if a new group must be provided access, the customer should re-install the RPASCE Client using the same install properties file as before, and specify the new set of groups during the installation process.

Users Must be Present in RPASCE

Users created in OID must be created in the RPASCE domain as well. Users that are not present in RPASCE will see an error message when they try to log into the application. Therefore, to remove a user's access from the application, it is enough to remove the user from RPASCE.

It is recommended that the customer delete users from RPASCE if they have been deleted from the authentication system.

RPASCE supports adding users through an interactive UI component (accessible only by administration users), and the bulk addition of users via an xml-format file (described in the RPASCE Online Administration Guide). This is transmitted through the same FTP interface used for other bulk data load tasks.

Authorization

Authorization refers to the selective provisioning of data and the functional access to different classes of users. There is no external configuration for this. Authorization data is managed within the RPAS CE application. To administer authorizations, the customer has to use the RPAS CE Client UI itself.

There are two authorization roles in RPASCE: admin and non-admin. After the server installation, a bootstrap admin user can be added to the RPASCE domain. This allows the addition of other users (admin and non-admin) through the RPAS CE Client UI. It is also possible to add users to RPASCE in bulk using a command line utility.

Note that the user groups in the authentication system (OID) have nothing to do with authorization (as defined above). Rather, OID groups are meant to serve as a convenient way to provide or revoke application access to multiple users en masse.

Auditing

The RPASCE Client tracks users as they log in and log out. To enable this, the category common.security.level is set by default to INFO. This is in the file logconfig.properties, which is located in the installation directory. This setting provides an audit trail of user login and logout activities. The login/logout entries can be found in the log file edge.log.<date>.

Password Policies

Password policies must be implemented in the OID. Note the following:

- Automatically lock out after a certain number of failed login attempts.
- Password expiration may be enabled.
- A password reuse time can be set.

Browser Security

Note the following.

Update the browser when new versions are released; they often include new security features.

Check browser for built-in safety features.

Set Policy For Unattended PC Sessions

Users may try to access an unattended workstation while the user is still logged into the system. Users must never leave their workstation unattended while logged into the system because it makes the system accessible to others. Organizations must set a corporate policy for handling unattended PC sessions. Users must use the password-locked screen savers feature on all PCs.

Configuration

A few parameters in the RPASCE Client that have a bearing on the application security profile can be modified by the customer after installation. They are set to certain values that provide the maximum security possible. However, these factory settings may not necessarily work well in relation to a specific customer's needs. The entries in the following table list the parameters, explain what they mean, and describe the implications of changing them from the factory settings.

Table 2–1 Factory Settings

Name	Released Setting	Description
printexport.maximum.cells	200000	Print/export will work only if cells in question do not exceed this value in number. Higher values can cause the server to fail with an out-of-memory error. It must be set to lowest acceptable value.
serverloglevel	Error	This is the logging level of the RPASCE Server. It is set for the duration of the user session. Lower levels collect more information and may be required for tracking defects. However, this can severely degrade performance. It is therefore recommended that the log level only be set to the lower levels when there are repetitive defects to be identified.
session.timeout	35	This determines how long a session between the browser and the application server must be inactive before expiring. The value is in minutes. It must be set to the smallest value acceptable to users.

3

Compute Tier Security

This chapter contains information on security activities carried out in the Compute Tier.

User and Group Management

RPASCE allows administrators to assign users into distinct groups. A group is similar to a traditional database role in that it allows the administrator to configure authorization settings for several users at once. The main difference, however, is that user and group have a hierarchical relationship, where settings are always stored at the user level and group is a rollup of user. User groups are typically assigned based on a common business role such as Planners in order to facilitate managing the authorization settings at the group level.

The group that a user rolls up to is referred to as the primary group. A user can also be associated with other groups using the Other Groups property. The Other Groups property is not used for authorization purposes, but instead allows a user to save workbooks and formatting in a way that it is visible to users whose primary group is one of those Other Groups. This behavior is typically used by people who need to support other users rather than an end-user, for example, a team whose job is to set up the formatting for all of the other project groups.

When a user is added, a position is created for the user in the metadata dimension, User. Similarly, when a group is added, that group is assigned a position in the metadata dimension Group. The frequent adding and dropping of users and groups can eventually exhaust the list of available positions in these dimensions and will require the reindexing of these dimensions.

Additionally, when a user is added, a directory is created for the user in the /users directory of the domain root. In global domains, this directory is created in the master and in all subdomains. This directory serves as a workbook repository, as well as a cache for some metadata such as MRU lists. When a user is deleted, these directories, as well as any workbooks created by that user, will be deleted with the user.

Locking User Accounts

User accounts can be marked as locked by the domain administrator. This prevents the user from logging on with the RPASCE Client. The account remains locked until the administrator re-enables the account. The domain administrator can set or clear account lockouts by using the User Management utility or the Edit User workbook.

Authorization

This section deals with authorizing access.

Workbook Security

Currently, workbook access is either granted or denied. If users have been granted access to a workbook, they can open, modify, and commit the workbook. No distinction is made between read-write-commit, read-write, and read-only access. Workbook access is automatically granted to the user who built it, and it may be shared with multiple groups or the world.

For guidance on assigning permissions to workbooks by role and group, see the Implementation Considerations chapter, section "Security," of each RPAS Application's Implementation Guide. All recommendations in the guides are for the GA solution. If a customer chooses to customize permissions, keep in mind that the Principle of Least Privilege: only provides users with enough permissions to do their job and nothing more.

Note: A user must have access to the workbook template in order to access the workbook, even if the workbook has world or group access rights.

Users with administrator status automatically have access to all workbook templates. By default, administrators have access to all workbooks that are saved with world access. If a workbook is saved with group access, administrators can only access the workbook if they are members of the default user group of the user who saved the workbook.

The Open dialog box initially shows only workbooks owned by the current user and in domains for which the user has position level security access. This is not the same as workbook access, however, and a user may have access to workbooks saved by others in other domains by using View > Other Domains in the Open dialog box by others Word or Group.

Another aspect of workbook security is the ability to set limits for the number of workbooks that a user can have saved at any given time. Limits can be set for a user per template, for a user group per template, or for a template for all users. The limits are evaluated in the above order, which means that a limit defined at user-template overrides any values defined at group-template or template. If the above limits are not defined, the default value is one billion.

The limits are checked when the workbook build process is initiated. When the limit is reached, an error message displays informing the user that the workbook build process cannot complete because the limit has been reached. The message also lets the user know what that limit is. The wizard process then terminates.

Administrative users have full access to all workbook templates, regardless of the access rights that other administrative users may assign to them in the Security workbook. The administrative user can build the Security workbook to change the access right back, so the nominal assignment does not matter for administrative users.

Non-administrative users do not have access to the Security template and User Administration template groups even if the administrator inadvertently assigns them access rights.

Measure Level Security

Measures have access rights; these are read-write, read-only, or denied. Measures that are read-write or read-only may be selected in the extra measures and insert measure dialogs. RPASCE ensures that read-only measures are not editable by the user and the presence of read-only measures does not affect the ability to commit a workbook.

Measure security can be specified and changed through the Security Administration workbook. The Measure Rights view allows Read Only, Deny, or Read/Write access to a measure to be specified for each user.

A workbook template can override the security of a measure, but it can only narrow the security of that measure. For example, a measure can have read-write access for a user and a template can specify that all users have read-only access to the measure when a workbook is built. However, if the measure security is read-only, the template cannot expand the security of that measure to read-write. Measures that are explicitly made read-only by a workbook template are not expanded to read-write access by RPASCE.

Position Level Security

Position Level Security allows access control for dimensions on a position-by-position basis. This capability is completely optional. If position level security is not explicitly defined and configured, all users in a domain have access to all positions in all hierarchies. After the position level security is defined, access to a position can be granted or denied for individual users, users in a group, or for all users.

Position level security can be defined at levels (dimensions) at or above base (such as class in the product hierarchy) in any hierarchy other than calendar. As positions are added at a level/dimension lower in the hierarchy than where the position level security is maintained, access to those positions is automatically granted if a user has access to the parent position. In other words, if security is maintained at the subclass level, users are automatically granted access to all the SKUs in a given subclass if they have access to that subclass. This includes those that were added after security was established.

Exactly one dimension in each hierarchy can be defined as the security dimension for the hierarchy. If a security dimension is defined for the hierarchy, all dimensions in the hierarchy have position level security enabled, but position security is set at or above the designated dimension. For instance, if the class dimension is designated as the security dimension, an administrator can maintain access to positions in the class dimension or at any level above class.

The enabling of position level security as well as the specification of the dimension at which position level security will be maintained are managed within the configuration used to define the domain. The RPASCE Configuration Tools provide the ability to do this configuration within the Hierarchy Definition Tool.

Additionally, position level security can be enabled on a domain by using the hierarchyMgr utility. This utility allows the specification of the security dimension without requiring modifications to the domain's configuration and the application of a domain content patch through the rpasInstall process. For more information on the use of the hierarchyMgr utility, consult the RPASCE Online Administration Guide.

After a security dimension is defined for a hierarchy, all users in the domain default to having access to all positions in any dimension in the hierarchy. Additionally, users automatically have access to newly added positions to a domain.

The Security Administration workbook is used to control position access for individual users, user groups, or all users (referred to as world or default access).

Three views are provided in this workbook for each hierarchy with a defined security dimension. The default view controls access to positions for all users (for instance, Prod Security Default); one view controls access to positions by user group (for instance, Prod Security Group); and the last view controls access to positions by individual users (for instance, Prod Security User).

Access must be granted at all levels for a user to have access to a position. This means a position must have a value of true at the levels default/world, group, and user. Table 3–1 demonstrates how access is granted or denied based on all combinations of settings. In the table, Denied = false and Granted = true. Based on the combination of settings, a user is either granted or denied access.

Table 3–1 Granting Access

User	User Group	World	Resulting Access
Denied	Denied	Denied	Denied
Denied	Denied	Granted	Denied
Denied	Granted	Denied	Denied
Granted	Denied	Denied	Denied
Denied	Granted	Granted	Denied
Granted	Denied	Granted	Denied
Granted	Granted	Denied	Denied
Granted	Granted	Granted	Granted

Position-level security is used when a user selects positions in the wizard process before building a workbook. Only positions to which a user has access are available for selection in the 2-tree, which are then included in the build of the workbook.

Note that position-level security, when used for a global domain environment on the same dimension on which it is partitioned, is used to guide a user to the domain or domains that the user has access to. If a user only has access to positions within a single local domain, that user will be guided there on New Workbook. If a user has access to more than one, that user will be asked and can choose based on partition-level positions.

Similarly, Open by default only lists workbooks from those domains, and a user is only shown alert counts from those domains.

Setting Proper Resource Limits

This section specifies how to set resource limits.

WorkbookTemplate Limits Views

The Workbook Template Limit views are used to limit the number of workbooks that the user can have saved. Limits can be set for a user per template, for a user group per template, or for a template for all users. The limits are evaluated in the above order, which means a limit defined in a user-template overrides any values defined at group-template or template. If the above limits are not defined, the default value is one billion, but it is not displayed in the workbook.

The limits are checked when the user begins the workbook build process. If the limit has been reached, an error message appears that informs the user that the workbook build process cannot complete because the limit has been reached. The wizard process then terminates.

Max Domain Session Limit View

The Max Domain Session Limit view is used to limit the number of user sessions that can be attached to a single domain by all users of that domain. The limit is set at the domain level. In a global domain environment, the same limit is applied individually to each local domain and the master domain.

This limit is checked during user login. If the limit has been reached, an error message appears to inform the user that the login has failed because this limit has been reached.

Max User Session Limit View

The Max User Session Limit view is used to limit the number of concurrent user sessions that can be attached to a single domain by the same user at the same time. The limit is set per user so that the administrator can control the maximum number of concurrent sessions that are allowed for an individual user. In a global domain environment, the same limit is applied individually to each local domain and the master domain.

This limit is checked during user login. If the limit has been reached, an error message appears to inform the user that the login has failed because this limit has been reached.

Information on how to set these limits can be found in RPASCE Online Administration Guide.

Dimension Modification Rights View

The Dimension Modification Rights view allows the administrator to determine which user defined dimensions, if any, a user can modify by using the Hierarchy Maintenance Workbook. The view contains a check box for each available user and dimension combination. A check mark in the cell indicates that the user is permitted to modify the specified user defined dimension. A check mark on the regular dimension has no affect. After changes are made to a user's dimension modification rights, they must be committed before they take effect.

Managing Sensitive Data

While RPASCE can be configured to store any type of data, it is designed to be used with sales history, inventory, and other business-related information with low security requirements. It is not intended to be used with any sensitive data, such as personally identifiable information or credit card information. It does not have any mechanisms to protect this data, such as encryption, and therefore must not be used in this manner.

Online Administration Tools

In order to be able to run and schedule administrative tasks in a cloud environment where the administrator has no access to the back-end servers, RPASCE Online Administration Tools provide an interface that allows authorized users to launch back-end processes from the RPASCE UI. It also provides a dashboard-like interface for the administrator to monitor the status of the tasks whose requests have been submitted.

Since the Administrator can launch processes in the back-end, albeit in a limited fashion, proper RPASCE server configuration is required to mitigate any security risks.

Authorization

By default, any RPAS administrative users have access to all RPASCE Administration Tools templates. In order to limit access to those sensitive templates, template security for RPASCE administrative users can be enabled in the domain

Auditing

All administrative tasks have a dedicated directory under the tasks folder of the domain. This directory contains the configuration, scheduling, and logging information of the task and can be used for auditing purpose. After a task is completed, its audit log is available through the Online Administration Dashboard. The number of successful or failed tasks whose logs are available through the dashboard is controlled by two domain properties:

- task_failed_limit: the number of failed tasks to be retained.
- task_success_limit: the number of successful tasks to be retained

4

Domain Security

This chapter of the security guide covers domain creation and maintenance.

Configuration Management

The process of RPASCE application configuration can be performed by an RPASCE administrator, an application expert, a consultant or a third-party implementation team. In all cases, the process of creating or modifying the configuration of an RPASCE application is performed using a stand-alone Java application known as the RPASCE Configuration Tools.

The RPASCE Configuration Tools work with an XML representation of the content of a domain known as the domain configuration. Using the Configuration Tools, a domain configuration can be inspected and modified. The configuration is then used as an input to the rpasInstall process, which creates and modifies RPASCE domains.

Because the RPASCE Configuration Tools are supported only on the Windows platform, there is a need to manage the transfer of that configuration between the system being used for the configuration and the system on which the RPASCE domain will be built and maintained.

Although the configuration itself does not contain any sensitive information, it does contain information about the meta-data of the domain and the processes used to maintain and modify that domain data. As such, it is prudent to secure the representation of the domain contained within the configuration.

To that end, there are three areas in which the security of a configuration can be discussed. These areas are:

- Upon the system on which the configuration process is performed.
- Upon the system on which the RPASCE domain is deployed.
- Upon the transfer of the configuration between the above two systems.

In each of these areas, precautions can be taken to maintain the integrity and confidentiality of the information represented within the configuration.

Securing the Configuration System

As the RPAS Configuration Tools do not interact directly with an RPAS domain, they cannot be used to inspect or modify domain information. However, because the configuration describes information about the information in the domain and the processes used to maintain and modify that information, it should be viewed as proprietary information. As such it should be subjected to the appropriate considerations employed to protect other proprietary information present on user systems.

The considerations include safeguarding the physical security of systems that store proprietary information, encryption of storage devices for these systems and limiting risk of exposure through controlling access to the information contained within the configuration.

Securing the Deployment System

.Once uploaded to the OCI environment, the configuration is protected by the same safeguards present to secure all domain resources residing within the host environment. No additional protections are required.

Securing the Transfer of Configurations

Configuration is performed on one or more users' individual systems. In order to build or update an RPAS domain with that configuration, it is necessary to transfer the configuration to the system upon which the domain will be deployed. This transport is accomplished through use of the SFTP upload process that is documented for data file upload and is described therein.

Dynamic Position Maintenance

The creation of positions within the dimensions of an RPAS domain is a process that is performed as part of an off-line process managed through the loadHier utility. However, the business processes performed by some RPAS applications make deferring position creation and management to an off-line process unacceptable.

Dynamic Position Maintenance (DPM) allows user to create and manage certain positions in an online process while working within a workbook. Users can create additional positions within constraints based on domain security settings and the workbook configuration and enforced by the RPAS Server instance.

Users can also modify and or delete existing positions created through DPM operations within constraints based on domain security settings and the workbook configuration and enforced by the RPAS Server instance.

Users are not allowed to modify or delete positions which the domain's security settings do not grant them access to; they may also not modify positions not allowed by the configuration of the workbook in which they are working. Finally, changes to formal positions managed through the loadhier process cannot by modified in any circumstances through DPM operations.

Enabling DPM functionality within a workbook involves the following process:

1. Configurator must enable DPM on particular dimensions on the domain.
2. Configurator must enable DPM on the specific workbook template.
3. Configurator or system administrator must ensure there is enough space to accommodate the volume of DPM position given by the bitsize of the dimension.
4. Administrator must give WRITE permission on that workbook template to the user.

When a user creates DPM positions, they are treated as temporary positions; loadHier does not update these positions. A command line utility informalPositionMgr is available for the purpose of:

1. When a user has finalized its information and wants to convert them to normal positions.
2. Application involves creating a very large number of DPM positions.

Like all RPAS server utilities. This command line utility should only have execution rights granted to system administrators.

RPAS Maintenance

Domain maintenance is a periodic operation that needs to be performed by the administrator. Its frequency depends on the degree to which the domain is subjected to hierarchy changes across time. Many of these operations can improve overall performance of data access operations - this can result in fewer contention issues which improves accessibility.

In addition, many of these operations involve removing data from the domain when that data is no longer needed by the operations being performed by the domain. This periodic cleansing serves to remove data from the system and addresses the need to retire data as a part of the data management life cycle. Some of the domain maintenance tasks that can be performed periodically are:

Purging Unused and Inactive Hierarchy Positions

All measure data within a domain is stored in either scalar or dimensional measures. As positions are introduced to the hierarchies of a domain, these positions become available for the storage of measure data. When a position is no longer needed by the domain, it can be purged. This purging, along with the use of the reindex domain, or optimize domain processes will result in the measure data associated with the retired positions being cleaned from the domain.

The purging process is performed by use of the loadHier utility purge operation. loadHier can be used to purge formal, informal, and user-defined positions from the listed hierarchies.

Cleanup of the Input and Processed Directories

RPASCE makes use of the loadhier and loadmeasure utilities to load information into the domain. These utilities read data in the form of text files that are staged to the input directory of the domain. Once the data in an input file is loaded, that file is moved to the processed sub-directory of the domain, where it is suffixed with a timestamp indicating the date and time of load.

Periodic clean up of these processed files is advisable because, over a period of time, these files can occupy sizable and valuable diskspace. The RPASCE Online Administration interface provides a Clean Up task that includes an option to remove all files from the processed directory in the domain.

Reindexing Domain Arrays

Run the reindexDomain analyze option from the master domain on individual hier/dims periodically to check whether a particular hier/dim requires a bitsize increase or whether it needs to be defragged. If hierarchy operations are frequent enough and if the above check is not made, then the size of the hier/dim and the available list of physical ids may not be sufficient enough to accommodate and allocate for the incoming hierarchy load request. This can result in a loadhier failure.

ReindexDomain also reshapes arrays, and a periodical run, in conjunction with the use of hierarchy purging, will remove inactive physical IDs and can potentially reduce the size of the domain arrays and remove unneeded data from the domain.

Optimizing Domain Arrays

Run optimizeDomain periodically from the master domain to improve performance and to minimize the space required by the domain data. Optimize domain has options to selectively defrag domain data based on database fragmentation and, in conjunction with hierarchy purging, to clean up domain data that is no longer required by the system.

A detailed description of LoadHier, ReindexDomain, and OptimizeDomain can be found in the RPASCE Online Administration Guide.

5

RPASCE Integration

This chapter covers integrating information across multiple RPASCE domains.

Data and Metadata Integration

The client/server interactions of RPAS CE define how users may access the system but are not effective for larger scale modification of the data of the system. To allow for these operations, RPASCE supports bulk data load and export operations. RPAS CE supports only file-based integration. These files are provided to and retrieved from the system through the use of an SFTP server that is part of the provisioned environment.

Integrating User Information

The RPASCE Platform supports the bulk creation of user accounts as a part of the domain build process. This bulk creation is accomplished by supplying a users.xml document with the other configuration inputs provided for the domain build.

The information contained within the supplied file is used to create a set of users and user groups within the RPASCE domain as a convenience; subsequent user maintenance is performed using the administrative user management templates. Note that user accounts created in this fashion will not have access to the system until they are provisioned within the OID. See the individual application Administrative Guides for information on creating and maintaining users in the OID.

Integrating Dimension and Measure Data

The RPASCE platform stores data within an embedded BTree database located within the domain on the file system. As such, it is necessary to manage the integration of the data within an RPASCE domain with other domains or with outside systems through a set of data import and export operations.

The primary operations used for this are the loadhier and loadmeasure utilities for importing data and the exportHier and exportmeasure utilities for exporting data. These operations can be performed either directly through scheduling a task in the Online Administration Tool interface or indirectly through the RPASCE batch framework.

The RPASCE platform supports the importing of data from and exporting of data to text files. These files provide an efficient method of moving large amounts of data into or out of an RPASCE domain. Based on configuration options for these tasks, the input and output files will be transferred via the SFTP server (for integration with non-cloud applications) or via an internal (single-tenant) file holding area for integration between multiple Oracle Cloud applications.

Details on secure access to the SFTP server, including instructions for setting up SSH keys, may be found in the Nightly Batch File Uploads section of each cloud application's Administration Guide.

6

Extending and Customizing Products

RPASCE allows the extension of the calculation capabilities of the Server component through the creation of custom calculation expressions. Calculations that modify customer data in the system are defined in an expression language; when processing customer data, a component of the Server known as the Calculation Engine performs updates according to the expressions defined within the application.

The expression language contains a predefined set of calculation primitives, such as arithmetic operations, and a set of predefined functions that perform more complex operations on the data. It is possible for a customer to extend this set of functions to provide unique methods for evaluating expressions and performing calculations through the creation of a Java Special Expression.

In order to maintain the security of the system, the execution of Java Special Expressions is tightly constrained. JVMs in which these expressions are run are created with the Java Security Manager installed with a security policy that grants no privileges to externally supplied code.

As a result, any operation attempted by externally supplied code that attempts to access any privileged resource, such as the file system, network, or even internal JVM resources such as class loaders, execution threads and executor services, or internal system properties will be vetoed by the Java Security Manager and will result in a SecurityException.

This exception will prevent the execution of the privileged action and should an exception halt the execution of externally authored code result in the halting of a Java Special Expression, a notification to the application monitoring team will be generated by the system.

Details about the security policy imposed on Java Special Expressions can be found within the *Oracle Retail Predictive Application Server RPASCE Extension Development Guide*.