Oracle® Communications Pricing Design Center

Security Guide

Release 11.2

E97176-01

July 2018

ORACLE®

Oracle Communications Pricing Design Center Security Guide, Release 11.2

E97176-01

Contents

Preface

This document provides guidelines and recommendations for setting up Oracle Communications Pricing Design Center (PDC) and its components in a secure configuration.

Audience

This document is intended for system administrators, database administrators, and developers.

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.

1

Pricing Design Center Security Overview

This chapter provides an overview of Oracle Communications Pricing Design Center (PDC) 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 such as SSL, and secure passwords.

  See "Performing a Secure Pricing Design Center Installation" 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," article on the Oracle Technology Web site:

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

Understanding the Pricing Design Center Environment

When planning your PDC implementation, consider the following:

- **Which resources need to be protected?**

  For example, you need to protect your pricing data, such as your bundle configurations.
- **Who are you protecting data from?**

  For example, if your business is planning to roll out new services and pricing data needs to be protected from your competition. Someone in your organization might need to access to your pricing data to manage it. You can analyze your process workflows to determine who needs that access and make sure the data remains protected.

- **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.

Oracle Security Documentation

PDC uses other Oracle products, such as Oracle Database and Oracle WebLogic Server.

See the following documents for more information:

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

Oracle documentation is available from the Oracle Technology Network Web site:

`http://docs.oracle.com`

2

Performing a Secure Pricing Design Center Installation

This chapter describes recommended deployment configurations for your Oracle Communications Pricing Design Center (PDC) installation that enhance security.

For information about installing PDC, see *PDC Installation and System Administration Guide*.

Recommended Installation Mode

You can install PDC in the following modes:

- Silent
- Secured

The silent installation is not meant for production environments, and it should be used only in test environments for setting up quickly or backing up the properties for later use in another test environment.

The secured installation is the only recommended option for production environments. See "Installing Pricing Design Center" for more information.

Operating System Security

PDC is supported on Linux 6UL6+ and 7UL2+ (both Oracle Enterprise Linux and Red Hat Enterprise Linux) and Oracle Solaris for SPARC (10 Update 4+ and 11 Update 3+). See the following documents for more information:

- Guide to the Secure Configuration of Red Hat Enterprise Linux 6 and 7 at

  `http://docs.redhat.com`

- Hardening Tips for the Red Hat Enterprise Linux 6 and 7 at

  `http://docs.redhat.com`

- Oracle Solaris 10 and 11 System Hardening References at

  `http://docs.oracle.com`

Installing Pricing Design Center

This section describes the security configurations during pre-installation and installation of PDC.

Pre-Installation

Perform the following pre-installation tasks:

- Verify that you have Oracle WebLogic Server installed.
- Enable SSL for the target WebLogic server domain, configure the server keystore certificate, and then get the client keystore trusted certificate (**.jks** file). You provide the path to this client-side keystore file during PDC installation to enable secure communication for PDC.
- If SSL is already enabled, ensure that the keystore file is created in a secure drive and access is strictly limited to the user account.
- Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer. See the Oracle Database documentation for advanced security configuration parameters. This is required for a PDC installer to make a secured (encrypted) database connection over the network. For more details, see *Oracle Database Advanced Security Administrator's Guide 12c Release*.
- Verify that you have JDK 1.8.0_172 or later installed.

Installation

- During PDC installation, select SSL mode and provide the client keystore certificate (**.jks** file) for connecting to a WebLogic server over SSL.
- The following logs are generated after the PDC installation.

  Location: **oraInventory/logs/**

  The default location of the **oraInventory** directory is in the **/etc/oraInst.loc** (Linux) file or the **/var/opt/oracle/oraInst.loc** (Solaris) file.

```
-rw-r-----  1 user1 eng  480058 Aug 15 09:25 installActions2011-08-15_
08-06-57AM.log
-rw-r-----  1 user1 eng    2384 Aug 15 10:33 dbScripts2011-08-15_10-32-00AM.log
-rw-r-----  1 user1 eng  124268 Aug 15 10:33 oraInstall2011-08-15_
10-27-07AM.err
```

  installAction*TimeStamp***.log** and **oraInstall***TimeStamp***.err** will have details in clear-text form entered in the PDC installation wizards. Passwords entered in the wizard are not logged in any of the PDC installation logs. Delete these installation log files if you do not need them for future reference, otherwise protect them appropriately if you do require them. These log files are created with the file level permission 640 (owner can read/write, group members can read, others cannot do anything) by default.

Post-Installation Configuration

- PDC user permissions depend on the group the user belongs to. The following groups are created in the WebLogic server during PDC installation:
  - Pricing Design Admin
  - Pricing Reviewer
  - Pricing Analyst
  - Migration Admin

The users belonging to the Pricing Design Admin group have read and write access and can perform any kind of operation from the PDC UI.

The users belonging to the Pricing Reviewer group have read-only access to the pricing and setup components.

The users belonging to the Pricing Analyst group have read and write access to all pricing components and read-only access to setup components.

The users belonging to the Migration Admin group can migrate pricing data from the BRM database to the PDC database.

None of the users by default is authorized to access PDC. The WebLogic server administrator must create an account for each intended user by creating the user in the WebLogic Server Administration Console and adding the user to one of the above groups depending on the user role.

- Do not use your browser's Remember Password feature for the WebLogic Server Administration Console URL. Always enter the WebLogic server user name and password manually in the login page, as a precaution.

Managing Cookies

Oracle recommends deploying PDC only on SSL, which encrypts sensitive data, thus eliminating problems like session stealing.

Using Secure Cookies

A common Web security problem is session stealing. This happens when an attacker manages to get a copy of your session cookie, generally while the cookie is being transmitted over the network. This can only happen when the data is being sent in clear-text format; that is, the cookie is not encrypted.

WebLogic Server allows a user to securely access HTTPS resources in a session that was initiated using HTTP, without loss of session data.

To use secure cookies:

1. Open the *MW_Home*/**user_projects/domains/***Domain_Name*/**config/config.xml** file.

   where:

   - *MW_Home* is the directory in which the Oracle Middleware components are installed.
   - *Domain_Name* is the name of the domain you are configuring.

2. Add **AuthCookieEnabled="true"** to the **<WebServer>** element.

   ```
   <WebServer Name="myserver" AuthCookieEnabled="true"/>.
   ```

You can also set this entry using the WebLogic Server Administration Console:

1. Log in to WebLogic Server Administration Console.

   The home page appears.

2. In the **Domain Configurations** section, under **Domain**, click **Domain**.

   The Settings for *Domain_Name* page appears.

3. Click the **Web Applications** tab.
4. Verify that the **Auth Cookie Enabled** check box is selected.
5. Click **Save**.

By default, the **Auth Cookie Enabled** check box is selected, but it is not present in the **config.xml** file. If you deselect it, the **<AuthCookieEnabled>** element is added to the **config.xml** file.

Setting **AuthCookieEnabled** to **true**, which is the default setting, causes the WebLogic Server instance to send a new secure cookie, _WL_AUTHCOOKIE_JSESSIONID, to the browser when authenticating through an HTTPS connection. After the secure cookie is set, the session is allowed to access other security-constrained HTTPS resources only if the cookie is sent from the browser.

For more information, see "Using Secure Cookies to Prevent Session Stealing" on the Oracle Technology Network Web site:

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/security/thin_client.html#wp1053780

Oracle recommends keeping cookies enabled in the browser. Disabling cookies in the browser disables several features, such as Help.

Configuring the Session Timeout

The default session timeout in PDC is 10 minutes. The WebLogic Server administrator can change this value after deployment by doing the following:

1. Log in to WebLogic Server Administration Console.
2. In the **Domain Structure** section, click **Deployments**.
3. Click on the application **PricingDesignCenter** deployed as type Enterprise Application.

   The deployment settings for **PricingDesignCenter** appear.
4. Click the **Configuration** tab.
5. Set **Session Timeout (in seconds):** to the new timeout value, in seconds.
6. Click the **Overview** tab.
7. In the Modules and Components table, click **PricingDesignCenter**.
8. Click the **Configuration** tab.
9. Set **Session Timeout (in seconds)**: to the same timeout value, in seconds, set in step 5.
10. Click **Save**.

    If no deployment plan is created, WebLogic Server creates one with the above changes and prompts you to save the deployment plan. Provide the name and path for the deployment plan and click **OK**.
11. In the **Domain Structure** section, click **Deployments**.
12. Select the application **PricingDesignCenter** deployed as type Enterprise Application.

    The **Update** button is enabled.
13. Click **Update**.
14. Select **Update this application in place with new deployment plan changes**.
15. Set **Deployment plan path** to the deployment plan created in steps 2 through 10. Click the **Change Path** button to browse to the file.
16. Click **Next**.

17. Click **Finish**.
18. Restart WebLogic Server.
19. Verify your changes by doing the following:
    a. Log in to WebLogic Server Administration Console.
    b. In the **Domain Structure** section, click **Deployments**.
    c. Click on the application **PricingDesignCenter** deployed as type Enterprise Application.

       The deployment settings for **PricingDesignCenter** appear.
    d. Click the **Configuration** tab.
    e. Verify that **Session Timeout (in seconds):** is set to the value you have provided.

For more information, see "Configuring Applications for Production Deployment" on the Oracle Technology Network Web site:

http://download.oracle.com/docs/cd/E12840_01/wls/docs103/deployment/config.html

Managing File Permissions

- Following are the default permissions set for the installed files:
  - rw------- 600 (for all nonexecutable files)
  - rwx------ 700 (for all executable files)

  Permissions are set to the lowest possible level, and the WebLogic Server administrator can add or revoke permissions. Oracle recommends keeping the permissions as restrictive as possible, as per your business needs.
- The WebLogic Server configuration (JMS, JDBC, etc) file, **config.xml**, in the domain's configuration directory should be protected with proper permissions.
- Output files generated by the export utility should be stored in a protected directory because it may contain sensitive pricing information.

Uninstalling Pricing Design Center

The following files remain in the system after uninstalling PDC:

- Install logs:

  Location: **oraInventory/logs/**

```
-rw-r-----  1 user1 eng  480058 Aug 15 09:25 installActions2011-08-15_
08-06-57AM.log
-rw-r-----  1 user1 eng       0 Aug 15 10:27 oraInstall2011-08-15_
10-27-07AM.out
-rw-r-----  1 user1 eng    2384 Aug 15 10:33 dbScripts2011-08-15_10-32-00AM.log
-rw-r-----  1 user1 eng  124268 Aug 15 10:33 oraInstall2011-08-15_
10-27-07AM.err
```

- *PDC_Home*/**oui/data.properties**: This file is used to auto-populate the data during re-installs.

Delete these files manually if you do not need them or protect them appropriately if they are required for future reference.

These files are created with the file permission 640 (owner can read/write, group members can read, others cannot do anything) by default.

Managing Passwords in PDC

When you install PDC, the passwords that you enter for the WebLogic Server domain, the PDC user, the transformation cross-reference database, the migration cross-reference database, and the BRM database are automatically encrypted. These encrypted passwords are stored in the PDC utility configuration files. The encryption keys for the encrypted passwords are stored in a keystore.

You use the **encrypt** utility to update the encrypted passwords in the PDC utility configuration files. See the discussion about changing encrypted passwords in the configuration files in *PDC Installation and System Administration Guide* for more information.

About the Keystore

A keystore is a file-based credential store that contains the encryption keys for the encrypted passwords. In PDC, the **pdc.jks** file is used as the keystore.

Each encryption key in a keystore has an alias key and is password protected. The keystore is also password protected.

The PDC Installer prompts you to enter the following when you install PDC and BRM Integration Pack:

- The encryption key password for accessing the PDC alias key in the keystore.
- The password used for accessing the keystore (**pdc.jks**).

The PDC Installer creates the **pdc.jks** file in the following locations:

- For PDC: *PDC_Home***/apps/conf**
- For BRM Integration Pack: *BRM_Integration_Pack_Home***/apps/conf**

The **pdc.jks** file is used by the following utilities:

- **ImportExportPricing**
- **SyncPDC**
- **BRETransformer** and **RRETransformer** (transformation engines)
- **MigrateBRMPricing**

When you run any of these utilities, the utility gets the encrypted password from its configuration file and prompts you for the encryption key password to access the encryption keys from the **pdc.jks** file. The utility then uses the encryption key from the **pdc.jks** file to decrypt the encrypted password.

For more information about the PDC utilities and their corresponding configuration files, see *PDC User's Guide* and *PDC Pricing Migration Guide*.

A

Secure Deployment Checklist

Follow this checklist to deploy your Oracle Communications Pricing Design Center (PDC) securely.

1. Pre-installation steps:
   a. Enable SSL for the target Oracle WebLogic Server domain.
   b. Configure the server keystore certificate and get the client keystore trusted certificate.
   c. Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer.
   d. Ensure that Oracle JDK 1.8.0_172 or later is installed and configured with your PDC or WebLogic installation.
2. Installation steps:
   - Select SSL mode and provide the client keystore certificate (**.jks** file) for connecting to a WebLogic server over SSL.
3. Post-installation steps:
   a. If you do not need the installation log files, make sure to delete them.
   b. The WebLogic Server administrator will need to create PDC users based on the roles and privileges.
   c. Do not use your browser's remember password feature for the WebLogic Server Administration Console URL.
   d. Enable secure cookies.
   e. Verify that file permissions for the installed files are 600 for all non-executable files and 700 for all executable files.
4. Un-installation steps:
   - Delete the log files in *OracleInventory***/logs/** manually if you do not need them or protect them appropriately if they are required for further references. These log files have file permission 640 (owner can read/write, group members can read, others cannot do anything) by default.