## Contents

### Preface

<table>
<thead>
<tr>
<th>Audience</th>
<th>v</th>
</tr>
</thead>
<tbody>
<tr>
<td>Documentation Accessibility</td>
<td>v</td>
</tr>
<tr>
<td>Related Documents</td>
<td>v</td>
</tr>
</tbody>
</table>

### 1 Pipeline Configuration Center Security Overview

- Basic Security Considerations .......................................................... 1-1
- Understanding the PCC Environment .................................................. 1-1
- Oracle Security Documentation ......................................................... 1-2

### 2 Performing a Secure Pipeline Configuration Center Installation

- Recommended Installation Mode .......................................................... 2-1
- Operating System Security ....................................................................... 2-1
- Installing Pipeline Configuration Center .................................................. 2-2
  - Pre-Installation ...................................................................................... 2-2
  - Installation ............................................................................................ 2-2
- Post-Installation Configuration .............................................................. 2-2
  - Managing Cookies ................................................................................... 2-3
    - Using Secure Cookies ........................................................................... 2-3
    - Configuring the Session Timeout ......................................................... 2-4
  - Managing File Permissions ...................................................................... 2-5
    - Securing the Infranet.properties File ................................................. 2-5
  - Uninstalling PCC ................................................................................... 2-5

### A Secure Deployment Checklist
Preface

This guide provides guidelines and recommendations for setting up Oracle Communications Billing and Revenue Management (BRM) Pipeline Configuration Center (PCC) and its components in a secure configuration.

Audience

This guide 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 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, see the following:

- PCC Help for step-by-step instructions for configuring pipelines by using PCC.
- BRM PCC Installation and System Administration Guide for detailed instructions on how to install and administer PCC.
- BRM documentation for information about BRM and Pipeline Manager.
This chapter provides an overview of Oracle Communications Billing and Revenue Management (BRM) Pipeline Configuration Center (PCC) 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.

- **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 secure sockets layer (SSL), and secure passwords.

  See "Performing a Secure Pipeline Configuration 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:


Understanding the PCC Environment
When planning your PCC implementation, consider the following:

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

  You need to protect the data required for pipeline rating, such as event data record (EDR) container descriptions.

- **Who are you protecting data from?**

  For example, if your business is planning to roll out new post-paid services, you need to protect the required pricing data and rating strategies from your competitors. However, someone in your organization might need to access that pricing data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that 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.

Oracle Security Documentation

PCC 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
Performing a Secure Pipeline Configuration Center Installation

This chapter describes recommended deployment configurations for your Oracle Communications Billing and Revenue Management (BRM) Pipeline Configuration Center (PCC) installation that enhance security.

For information about installing PCC, see BRM PCC Installation and System Administration Guide.

Recommended Installation Mode

You can install PCC in the following modes:

- GUI mode
- Silent mode

Oracle recommends that you install PCC using secure sockets layer (SSL) in a production environment. See "Installing Pipeline Configuration Center" for more information.

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

Operating System Security

PCC is supported on Linux 5 UL3+ (both Oracle Linux and Red Hat Enterprise Linux), Oracle Solaris for SPARC (10 Update 4+), Windows XP (SP3) (browser only), and Windows 7 (browser only). See the following documents for more information:

- Oracle Solaris 10 System Hardening References, available at http://docs.oracle.com
Installing Pipeline Configuration Center

This section describes security configurations for pre-installation and installation of PCC.

Pre-Installation

Perform the following pre-installation tasks:

- Enable SSL for the target Oracle WebLogic Server server domain, configure the server keystore certificate, and get the client keystore trusted certificate (.jks file).
- If SSL is 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 the PCC installer to make a secured (encrypted) database connection over the network. For more information, see Oracle Database Advanced Security Administrator’s Guide 11g Release 1 (11.1), available at the following Web site:
  
  http://download.oracle.com/docs/cd/B28359_01/network.111/b28530/asojbdc.htm#i1006157

- Verify that you have JDK 1.6.0_33 or later installed.

Installation

- During the PCC installation, select SSL mode and provide the client keystore certificate (.jks file) for connecting to a WebLogic server over SSL.
- During PCC installation, the following log files are generated in the oraInventory/logs directory:
  - installActionTimeStampl.log
  - oraInstallTimeStampl.err
  - oraInstallTimeStampl.out
  - silentInstallTimeStampl.log (for silent mode installation)
  
  where TimeStamp is the date and time the log file was created.

installActionTimeStampl.log and oraInstallTimeStampl.err have details in clear text form entered in the PCC installation screens. Passwords entered in the screen are not logged in any of the PCC installation logs. Delete these log files if you do not need them for future reference; protect them appropriately if you do require them. By default, these log files are created with the file-level permission 640 (owner can read/write; group members can read; others cannot do anything).

Post-Installation Configuration

During the PCC installation, the PCC installer creates the Config Admin WebLogic Server group. Users belonging to this group have read and write access to perform all the tasks in PCC.

You can create a PCC user during or after the installation. When you create a user during the installation, the installer automatically adds the user to the Config Admin group.
To create a PCC user after installing PCC, use the WebLogic Administration Console to create a user and to add the user to the Config Admin group.

---

**Note:** Do not use your browser’s remember password feature for the WebLogic Administration Console URL. As a precaution, always enter the WebLogic server user name and password manually.

---

**Managing Cookies**

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

**Using Secure Cookies**

WebLogic Server enables 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 `WebLogic_Home/user_projects/domains/Domain_Name/config/config.xml` file.
   - Where:
     - `WebLogic_Home` is the directory in which you installed WebLogic Server.
     - `Domain_Name` is the name of the domain you are configuring.
   2. Add `AuthCookieEnabled="true"` to the `<WebServer>` element:

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

   **Note:** By default, `AuthCookieEnabled` is set to `true`. The secured cookies are enabled by default even if the `config.xml` file does not contain this entry. You can set `AuthCookieEnabled` to `false` to disable secured cookies. However, Oracle recommends not disabling it.

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

1. Log in to the WebLogic 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`, 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 the “Using Secure Cookies to Prevent Session Stealing” article 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 cookie settings enabled in the browser. Disabling cookies in the browser disables several other features, such as Help.

Configuring the Session Timeout

The default session timeout in PCC is 600 seconds. The WebLogic Server administrator can change this value as follows:

1. Log in to the WebLogic Administration Console.
2. In the Domain Structure panel, click Deployments.
   The Summary of Deployments page appears.
3. In the Deployments table, click PipelineConfigurationCenter.
   The Settings for PipelineConfigurationCenter page appears.
4. Click the Configuration tab.
5. In the Session Timeout (in seconds) field, enter a new timeout value in seconds.
6. Click the Overview tab.
7. In the Modules and Components table, click PCC-PCCViewController-context-root.
8. Click the Configuration tab.
9. In the Session Timeout (in seconds) field, enter the same timeout value, in seconds, that you entered in step 5.
10. Click Save.
   If no deployment plan is created, WebLogic Server creates one with the preceding 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 panel, click Deployments.
12. Select the PipelineConfigurationCenter check box.
13. Click Update.
   The Update Application Assistant starts.
14. Select the Update this application in place with new deployment plan changes option.
15. Set Deployment plan path to the deployment plan created in step 10. Use the Change Path button to browse to the file.
16. Click Next.
17. Click Finish.
19. Verify your changes by doing the following:
   a. Log in to the WebLogic Administration Console.
   b. In the Domain Structure panel, click Deployments.
c. Click **PipelineConfigurationCenter**.
The **Settings for PipelineConfigurationCenter** page appears.
d. Click the **Configuration** tab.
e. Verify that **Session Timeout (in seconds)** is set to the value you specified.

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

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

### Managing File Permissions

- The following default permissions are 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.

- Protect the WebLogic configuration (JMS, JDBC, and so on) file, `config.xml`, in the domain's `config` directory with proper permissions.

### Securing the Infranet.properties File

During the PCC installation, the installer creates the `PCC_Home/plan/AppFileOverrides/PCCView.war/Infranet.properties` file.

An **Infranet.properties** file is a configuration file that contains entries to control connections from Java applications to BRM. For more information about such files, see the BRM documentation set.

After the installation is complete, you add the BRM user name and password for connecting PCC to BRM to the PCC **Infranet.properties** file. See **BRM PCC Installation and System Administration Guide** for more information.

To secure this connection information, do the following:

- Encrypt the password by using the `pin_crypt_app` utility. See the BRM documentation for more information about the utility.
- Set the **Infranet.properties** file permissions to permit only specified system administrators to access the file.

### Uninstalling PCC

The following files remain in the system after PCC is uninstalled:

- **Install logs**
  
  The log files are in the `orainventory/logs` directory.
- **PCC_Home/oui/data.properties**

  This file is used to auto-populate the data during reinstalls.

  Delete these files manually if you do not need them, or protect them appropriately if they are required for further installations.

  By default, these files are created with the file-level permission 640 (owner can read/write; group members can read; others cannot do anything).
To deploy Oracle Communications Billing and Revenue Management (BRM) Pipeline Configuration Center (PCC) securely, follow this checklist:

1. Pre-installation steps:
   a. Enable secure sockets layer (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. Verify that you have JDK 1.6.0_33 or later installed and configured with your PCC/WebLogic Server installation.

2. Installation steps:
   a. 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, delete them.
   b. The WebLogic Server administrator must create PCC users based on the roles and privileges.
   c. Do not use your browser’s remember password feature for the WebLogic Administration Console URL.
   d. Enable secure cookies.
   e. Verify that file permissions for the installed files are 600 for all nonexecutable files and 700 for all executable files.

4. Uninstallation steps:
   a. Delete the log files in the \oraInventory\logs directory manually if you do not need them, or protect them appropriately if they are required for further installations.