Lab 6 – Installing an Application

At the end of this exercise, you should be able to:
- Use the administrative console to install an application
- Use a web browser to test the application
- Use the drag-and-drop function to deploy an application

The Plants By WebSphere sample uses a Derby database, which must be setup before running the application. The application assumes the Derby database will be installed in install_root/Derby/databases. Use the following commands to setup the Derby database before installing and running the Plants by WebSphere sample application:

```
cd install_root/Derby/databases

jar xf ../../samples/PlantsByWebSphere/Derby/PLANTSDB/pbw-db.jar
```

Section 1: Start the server and the administrative console

Use the WebSphere Application Server administrative console to install the PlantsByWebSphere application. Since the administrative console is an application that is running on the server, the server must be running before the administrative console is started.

Section 2: Create J2C authentication aliases

Most system resources must be able to authenticate to a registry. Data sources must be able to authenticate to the database server. Here the database is set up to use the local OS user registry.

Section 3: Create a JDBC provider and data sources for the application

If any resources that the application uses are not defined in the EAR file, you must define them. You can use the administrative console to define the resources. In this section, you create the data sources that the PlantsByWebSphere application requires. These data sources define how the application accesses the PLANTS database. You also create the JDBC provider under which the data source exists.

The **Component-managed authentication alias** involves creating a mapping from an alias name to the user name and password. This alias name is then specified administratively on the connection factory or data source. As the alias can be resolved in the application server only, the alias restricts authenticated access to applications that are running in the application server.

The **Container-managed authentication alias** works in much the same way as the component-managed alias, but the connection factory or data source must be looked up by using a resource-reference that specifies a resource-auth of container. As a consequence, for an application to retrieve the authenticated resource, the administrator must explicitly bind the resource-reference to the resource on deployment of the application.

Section 4: Install the PlantsByWebSphere enterprise application

The EAR file that you are installing can be on either the client computer or the server computer. The client computer runs the browser, and the server computer is the computer to which the client is connected. If you specify an EAR file on the client computer, select **Local file system**. Then, the administrative console uploads the EAR file to the computer on which the console is running and proceeds with application installation.

If you are using a browser on a remote location, select **Remote file system** and browse through the file system where the application server is running.

The **Fast Path** method limits the number of options that are shown, which simplifies the installation process. The **Detailed** method shows all the installation options, including the options with default values assigned.

If an EAR file is enhanced, the **Process embedded configuration** check box is selected by default. To ignore the application-scoped resources, the **Process embedded configuration** option must not be selected.

If this enhanced EAR file is installed with the **Process embedded configuration** checked, then various properties are set at the application scope level. Caution must be used when working with application scoped resources because they are not as clearly visible as resources set at higher level scopes.

- Application scoped resources are tied to a specific application. Enhanced EAR files include application resources.

- Settings that are made at the application scope level take precedence over the same settings that are set at a higher level scope, such as the cell or node levels.

- Application scoped resources are not available from scope selection menus.

It is problematic if an administrator is trying to troubleshoot a problem and is not aware that an application is enhanced. A setting at the application scope can cause a problem with the application. The administrator might review all the settings at the various scopes and never look at the application scope settings.

Section 5: Test the enterprise application

Test the application by accessing it with the WebSphere Application Server HTTP transport.

Section 6: Use a monitored directory to deploy an enterprise application

In this section, the new monitored directory feature is used to deploy an EAR file. This feature allows the deployment of an application by dragging, or copying, an EAR file into a monitored directory. The application is automatically installed and started.

The monitored directory feature is not enabled by default. The first step is to use the administrative console to enable the feature. This step creates the directory structure that the monitored directory feature uses.