WebSphere Application Server V7: Working with Profiles on z/OS Systems

The purpose of this chapter is to help you build your initial WebSphere® Application Server environment using the new WebSphere Customization Tools (WCT).

We cover the following topics:
- “Creating WebSphere environments” on page 2
- “Creating a deployment manager definition” on page 12
- “Creating the base application server definition” on page 43
- “Federating an application server” on page 65
- “Creating a job manager profile” on page 71
- “Creating an administrative agent profile” on page 81
Creating WebSphere environments

Configuring a WebSphere Application Server for z/OS® environment consists of setting up the configuration directory for the environment and making changes to the z/OS target system that pertain to the particular application serving environment. Configuring these application serving environments after product installation requires a fair amount of planning and coordination.

For example, when defining multiple deployment managers or application servers on a single machine or logical partition (LPAR), you need to ensure that the ports and names you select for each are unique and the z/OS environment variables, generated jobs, and so on, are all set up properly. We strongly recommend that you spend time planning the installation and if possible, first practice by configuring a standalone application server using the default options.

You use the WebSphere Application Server for z/OS Profile Management Tool (PMT) available with the WebSphere Customization Tools (new with V7) to configure WebSphere Application Server environments for the z/OS platform.

The PMT is a dialog driven tool that runs in the WebSphere Customization Tools. It is an Eclipse plug-in that allows you to perform the initial setup of WebSphere Application Server for z/OS cells and nodes. It provides the same functionality as the former ISPF dialogs plus additional features to help you.

The WCT itself does not create the cells and nodes; however, it creates batch jobs, scripts, and data files that you can use to perform WebSphere Application Server for z/OS customization tasks. These jobs, scripts, and data files form a customization definition on your workstation, which is then uploaded to z/OS where you submit the jobs as pictured in Figure 1 on page 3.
The WCT for z/OS is a workstation graphical tool that is used to generate the customized jobs used to create, migrate or augment a WAS z/OS configuration.

**Objective - creation of customized jobs for the purpose of creating or modifying a configuration**

**Figure 1 The WCT configuration flow**

**Note:** The ISPF dialogs were deprecated in WebSphere Application Server Version 6.1, and as of WebSphere Application Server Version 7.0, the ISPF panels are no longer available.

**Review the documentation:**

The WebSphere Application Server Information Center contains planning topics for each WebSphere Application Server package that is tailored to each platform. This section gives you a high-level look at the planning tasks you need to perform.

If you are planning a WebSphere Application Server for z/OS environment, we strongly suggest that you review the installation planning material for z/OS platforms available at the WebSphere Application Server Information Center at the following URL:

The PMT requires that you have the WebSphere Customization Tools (WCT) application. For more information about how to download and install the WCT, see the following URL:

http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg24020368

For additional information about the function of the WCT, see the following document: *Introducing the WCT for WebSphere z/OS Version 7*, found at:

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS3357

A spreadsheet has been developed that can help you create and document your configuration variables. This spreadsheet can be downloaded from the following URL. Many of the values that you need to specify to the PMT tool can be planned using this spreadsheet:

http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS3341

Through the PMT, you can create environments for the following products:

- WebSphere Application Server for z/OS
- WebSphere DMZ secure proxy server for z/OS

**WebSphere Application Server for z/OS**

The PMT provides support to generate jobs to create the following WebSphere Application Server for z/OS environments:

- Create a cell environment consisting of a deployment manager and a federated application server.
- Create a management environment, which can be either:
  - A deployment manager
  - A job manager *(New in V7)*
  - An administrative agent *(New in V7)*
- Create a standalone application server environment.
- Create a managed (custom) node and federate it into an existing cell.
- Federate an application server.
WebSphere DMZ secure proxy server for z/OS

The DMZ secure proxy server for IBM® WebSphere Application Server installation allows you to install your proxy server in the demilitarized zone (DMZ), while reducing the security risk that might occur if you choose to install an application server in the DMZ to host a proxy server. The risk is reduced by removing any functionality from the application server that is not required to host the proxy servers, but that could pose a security risk. Installing the secure proxy server in the DMZ rather than the secured zone presents new security challenges. However, the secure proxy server is equipped with capabilities to provide protection from these challenges.

The PMT Version 7.0 provides support for the following WebSphere DMZ secure proxy server for z/OS environments:

- **Management:**
  Generates the customization jobs to create an administrative agent for the secure proxy server.

- **Secure proxy:**
  Generates the customization jobs to create a secure proxy server.

Getting started with the profile management tool

This section explains how to prepare and start the PMT. These steps are common for any type of profile.

To start the PMT, perform the following steps:

1. Start the WebSphere Customization Tools (WCT).
   
   On Windows®, you can start it from the Windows Start menu:
   
   **Start → All Programs → IBM WebSphere → WebSphere Customization Tools V7.0 → WebSphere Customization Tools**
   
   On Linux®, use the menus used to start your programs.

   For example, click **operating_system_menus_to_access_programs → IBM WebSphere → WebSphere Customization Tools V7.0.**
2. Click the **Welcome** tab. You are presented with the Welcome window shown in Figure 2.

![WebSphere Customization Tools welcome](image)

*Figure 2  WebSphere Customization Tools welcome*
3. Select the **Profile Management Tool (z/OS only)** option and click the button, **Launch Selected Tool**. You are presented with the PMT panel as shown in Figure 3.

![Profile Management Tool panel](image)

*Figure 3  Initial Profile Management Tool panel*
4. Create a new location by clicking the Add button (top right corner). The definitions containing the generated customization jobs will be stored at the location you define here:

a. Select **Create a new customization location** and give a name to the new location as shown in Figure 4.

**Note:** The PMT is compatible with WebSphere Application Server Version 6.1; therefore, for a single location you can create definitions for either WebSphere Application Server V6.1 or WebSphere Application Server V7.0.

b. Select **Version 7.0** and the corresponding folder for this location.

![Create the customization location](image)

*Figure 4  Create the customization location*

c. Click **Finish** to create this location.
The Profile Management Tool panel opens (Figure 5).

Figure 5  Profile management tool main panel
Using response files:

Each time you create a customization definition, it is stored in a directory in the selected customization location. A corresponding response file is generated in the same directory.

You can display this response file by switching to the Customization Response File tab in the previous panel (Figure 5). See the last tab in the bottom portion of the panel. You can use this response file when creating future profiles to populate the input fields with values contained in the response file.

Configure Additional Users:

If your daemon and control region adjunct processes have to run using different user IDs from the associated control region process, you should enable the following setting:

Click Window → Preferences → Profile Management Tool in WebSphere Customization Tools Version 7.0.0.1 or later, select Enable unique user IDs for daemon and adjunct, and click Apply.

With this setting, you get an additional panel when you build a customization definition that allows you to specify additional user IDs for processes relevant to the profile (that is, for the controller adjunct and daemon processes).
5. To begin a new customization definition, click **Create**. You are now presented with the panel (Figure 6) welcoming you to the Profile Management tool.

![Profile Management Tool](image.png)

*Figure 6  PMT Welcome panel*

6. Click **Next** to get started with creating profiles.

**Sample environment**

In this section, we demonstrate how to use the PMT to create a z/OS Network Deployment cell (deployment manager and application server). We chose this configuration, because it is representative and inclusive of the panels and steps that you will encounter with the other environments.
Figure 7 illustrates the flow that you go through in order to generate the jobs for this configuration.

We build the environment in three steps:
1. Create a deployment manager profile.
2. Create an application server profile.
3. Federate the application server to the deployment manager cell.

Creating a deployment manager definition

The first step in building the sample WebSphere environment is to create the deployment manager.

Creating the customization definition

To begin, run the profile management tool to create the custom definition:
1. Click Create on the Profile Management Tool main panel.

   The first panel that you see when you click Next on the Profile Management Tool Welcome panel prompts you to select the type of WebSphere environment that you want to create.
2. Select **Management** and click **Next** (Figure 8).

![Profile Management Tool 7.0](image)

*Figure 8  Environment selection panel*

3. Select **Deployment manager** and click **Next**.

4. The next window, Figure 9 on page 14, contains the following fields:
   
   – Customization definition name:
     
     Used to specify the customization profile you are about to create. This name is not transported to your host system.
   
   – Response file path name:
     
     Allows you to specify a saved file with values from a previously created configuration. Doing this populates the fields throughout the windows with the values that are contained in the response file. This field is optional.

Because it is the first time that you will be creating a profile, you probably do not have this file. A response file is written each time a z/OS customization definition is created, and its name is the customization definition name itself + `.responseFile` created under the root directory for the customization definition. Normally, you should specify a response file from a customization definition of the same type as you are about to define. However, a response file from a similar customization type can be used to pre-load most of the default values.
5. The next panel (Figure 10 on page 15) allows you to specify defaults for GID and UID values, name and user ID defaults based on a two character prefix that identifies the cell, and allows you to specify a default range for ports assigned to the process.
Figure 10 Specify default values

Click Next.
6. The next panel (Figure 11) asks you to specify a high-level qualifier for the target z/OS data sets that will contain the generated jobs and instructions.

![Profile Management Tool 7.0](image)

**Figure 11  Creating a deployment manager profile: Target Data Sets window**
The high-level qualifier can be composed of multiple qualifiers up to 39 characters. When a customization profile is uploaded on the target z/OS system, the generated jobs and files are written on a pair of data sets. The same data sets can be reused for a future installation; however, we strongly recommend you create a new pair of data sets for every new profile installation.

A good planning and naming convention is crucial when defining this type of information. As a best practice, try to set the high-level qualifier according to the version and release of WebSphere Application Server for z/OS, the task you are performing, and the cell (and, in some cases, the node name) you are configuring.

In this case, the following data sets will be created when the customization profile is uploaded to the target z/OS system:

- JVESER.WAS70.WPDMNODE.CNTL
- JVESER.WAS70.WPDMNODE.DATA

The CNTL data set is a partitioned data set with a fixed block 80-byte record that keeps the customization jobs. The DATA data set is a partitioned data set as well, but with variable length data to contain the other customization data.

Click Next.

**Note:** After the customization profile is created, the data set names cannot be changed, because all jobs are based on these data set names.
7. The next panel (Figure 12) contains the fields to configure common groups.

![Configure Common Groups](image)

*Figure 12  Deployment manager: Configure common groups*
The information that you need to provide for this panel is as follows:

- **WebSphere Application Server Configuration Group Information:**
  Used to specify the group name for the WebSphere Application Server administrator user ID and all server user IDs.

- **WebSphere Application Server Servant Group Information:**
  Used to connect all servant user IDs to this group. You can use it to assign subsystem permissions, such as DB2® authorizations, to all servants in the security domain.

- **WebSphere Application Server Local User Group Information:**
  Specify the local client group. This group provides minimal access to the cell.

- **WebSphere Application Server user ID home directory:**
  Specify a new or existing z/OS file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process. Note that this directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

Click **Next**.
8. The next panel (Figure 13) configures the common users.
– Common controller user ID:
  The user ID associated with all the control regions and the daemon. This user ID will also own all of the configuration file systems.
– Common servant user ID:
  The user ID associated with the servant regions.
– WebSphere Application Server administrator user ID:
  The initial WebSphere Application Server administrator. The ID must have the WebSphere Application Server configuration group as its default UNIX® System Services group. The UNIX System Services UID number for the administrator user ID is specified here, and must be a unique numeric value between 1 and 2,147,483,647.

Click **Next**.

9. The next panel (Figure 14) requests system and data set names.

![Profile Management Tool 7.0](image)

*Figure 14  Creating a deployment manager profile: System and Dataset names*

– System name: The system name of the target z/OS system.
– Sysplex name: The sysplex name of the target z/OS system.
Note: If you are not sure of the system and sysplex names for your target z/OS system, you can use the console command, D SYMBOLS, on the target z/OS system to display them.

- PROCLIB data set name: The PROCLIB data set where the WebSphere Application Server for z/OS cataloged procedures are to be added.

Click Next.

10. The next panel (Figure 15) requests the cell, node, and server names.

Figure 15  Deployment manager: Cell, Node and Server Names
– **Cell short name:**
  Identifies the cell to z/OS facilities, such as System Authorization Facility (SAF).

– **Cell long name:**
  The primary external identification of this WebSphere Application Server for this z/OS cell. This name identifies the cell as displayed through the administrative console.

– **Deployment manager short name:**
  The name that identifies the node to z/OS facilities, such as SAF.

– **Deployment manager long name:**
  The primary external identification of this WebSphere Application Server for the z/OS node. This name identifies the node as displayed through the administrative console.

– **Deployment manager server short name:**
  Identifies the server to z/OS facilities, such as SAF. The server short name is also used as the server JOBNAME.

– **Deployment manager server long name:**
  The name of the application server and the primary external identification of this WebSphere Application Server for the z/OS server. This name identifies the server as displayed through the administrative console.

– **Deployment manager cluster transition name:**
  The Workload Manager (WLM) application environment (WLM APPLENV) name for the deployment manager. If this is a server that is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are of the same cluster.

Click **Next**.

**New in V7:** With Version 7.0, the WebSphere Application Server LOADLIBs are located in the product filesystem instead of separate data sets as in Version 6.1. Therefore the STEPLIBs are not needed anymore. Consequently, in Version 7.0, the Z-member in PROCLIB disappears.
11. The next window (Figure 16) requests configuration file system information for your z/OS system. The file system can be either HFS or zFS. It is used to hold WebSphere Application Server configuration information.

![Configuration File System](image)

Figure 16  Deployment manager - configuration file system
– Mount point:
  The read/write HFS directory where application data and environment files are written. The customization process creates this mount point if it does not already exist.

– The directory path name relative to the mount point:
  Directory to be used for the deployment manager home directory.

– Data set name:
  The file system data set you will create and mount at the specified mount point above.

– Volume, or "*" for SMS:
  Specify either the DASD volume serial number to contain the above data set or "*" to let SMS select a volume. Using "*" requires that SMS automatic class selection (ACSTM) routines be in place to select the volume. If you do not have SMS set up to handle data set allocation automatically, list the volume explicitly.

– Primary allocation in cylinders:
  The initial size allocation for the configuration file system data set. In the application server, the total space needed for this data set increases with the size and number of the installed applications. The minimum suggested size is 250 cylinders (3390).

– Secondary allocation in cylinders:
  The size of each secondary extent. The minimum suggested size is 100 cylinders.

– File System type:
  Select to allocate and mount your configuration file system data set using as either HFS or zFS.

Click Next.

12. The next panel (Figure 17 on page 26) defines the product file system directory and allows you to set up an intermediate symbolic link (see Chapter 7, WebSphere Application Server for z/OS V7 administration for more information).

In the past, the intermediate symbolic links had to be set up manually.

**Recommendation:** Use intermediate symbolic links for flexibility when applying maintenance and running with different versions of the code.
Click **Next**.
13. Enter the job names, procedure names, and user IDs to use for each process in the panel shown in Figure 18.

![Deployment manager - processes](image.png)

**Figure 18  Deployment manager - processes**

- Deploy manager controller process:
  The job name is specified in the MVS START command JOBNAME parameter, associated with the control region. This is the same as the server short name and it cannot be changed during customization. The procedure name is the member name in your procedure library to start the control region. The User ID is the user ID associated with the control region.

- Deploy manager servant process:
  Specify the job name used by WLM to start the servant regions. This is set to the server short name, followed by the letter “S,” and it cannot be changed during customization. The procedure name is the member name in your procedure library to start the servant regions. The User ID is the user ID associated with the servant regions.

Click **Next**.
14. The next panel (Figure 19) requires you to specify the ports to use for each process. Planning is very important to avoid port conflicts, so be sure that you have all values you need in order to complete this panel.

![Profile Management Tool 7.0](image)

**Figure 19** Deployment manager - port values

Comparing the ports with V6.1, two additional ports have been added—the Administrative interprocess communication port as well as the DataPower® appliance manager secure inbound port.

After completing the required ports, click **Next**.

15. The next panel (Figure 20 on page 29) requests the location service daemon settings. The location daemon service is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the
CORBA-based location service agent that places sessions in a cell. All RMI/IIOP IORs (for example, enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

![Location Service Daemon Definitions](image)

*Figure 20  Location Service Daemon Definitions*
– Daemon home directory:
  The directory in which the location service daemon resides. This is set to the configuration file system mount point/Daemon and cannot be changed.

– Daemon job name:
  Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon. When configuring a new cell, be sure to choose a new daemon job name value. A server automatically starts the location service daemon if it is not already running.

– Procedure name:
  Member name in your procedure library to start location service daemon.

– IP name:
  The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses. The default is your node host name. In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name. Select the IP name for the location service daemon carefully. You can choose any name that you want, but, after being chosen, it is difficult to change, even in the middle of customization.

– Listen IP:
  The address at which the daemon listens. Select either * or a dotted IP address for this value.

– Port:
  Specify the port number on which the location service daemon listens.

– SSL port:
  The port number on which the location service daemon listens for SSL connections.

**Note:** Choose the IP name and port number carefully, because these are difficult to change, even in the middle of customization.

– Register daemon with WLM DNS check box:
  If you use the WLM DNS (connection optimization), you must register your location service daemon. Otherwise, do not register your location service daemon. Only one location service daemon per LPAR can register its domain name with WLM DNS; if you have multiple cells in the same LPAR and register more than one location service, it will fail to start.
Click **Next**.

16. The next panel allows you to enter SSL customization values as shown in Figure 21.

![Profile Management Tool 7.0](image)

*Figure 21  SSL Customization*

- **Certificate authority keylabel:**
  The name that identifies the certificate authority (CA) to be used in generating server certificates.

- **Generate certificate authority (CA) certificate check box:**
  Selected to generate a new CA certificate. Do not select this option to have an existing CA certificate generate server certificates.

- **Expiration date for certificates:**
  Used for any X509 Certificate Authority certificates created during customization, as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers. You must specify this even if you have not selected **Generate Certificate Authority (CA) certificate**.
– Default SAF keyring name:
  
The default name given to the RACF® keyring used by WebSphere Application Server for z/OS. The keyring names created for repertoires are all the same within a cell.

– Enable SSL on location service daemon check box:
  
  Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If selected, a RACF keyring will be generated for the location service daemon to use.

  After completing the required SSL information, click Next.

17. The next window allows you to select the user registry to be used for administrative security. You can choose from the following options:

– z/OS security product option: This option uses the z/OS system's SAF compliant security product, such as IBM RACF or equivalent, to manage WebSphere Application Server identities and authorization according to the following rules:
  
  • The SAF security database will be used as the WebSphere user repository.
  
  • SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
  
  • Digital certificates will be stored in the SAF security database.

  Note: Select the z/OS security product option if you are planning to use the SAF security database as your WebSphere Application Server registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking. For this security option, you must decide whether to set a security domain name, and choose an administrator user ID and an unauthenticated (guest) user ID.
WebSphere Application Server security option:

The WebSphere Application Server administrative security option is used to manage the Application Server identities and authorization according to these rules:

- A simple file-based user registry will be built as part of the customization process.
- Application-specific role binds will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

**Note:** Choose this option if you plan to use an LDAP or custom user registry without mapping to SAF user IDs. (The file-based user registry is not recommended for production use.)

No security:

Although it is not recommended, you can disable administrative security. If you choose this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually. You can enable security manually later via the administrative console or using Jython scripts.

Select an option and click **Next**. The next window that you see will depend on the security option you choose.

18. Figure 22 on page 34 shows the parameters to enter if you selected the z/OS security product option.
Figure 22  Setting z/OS security

- SAF profile prefix: (Formally known as Security domain identifier):
  This optional parameter is used to distinguish between APPL or EJBROLE profiles based on security domain name. It provides an alphanumeric security domain name of one to eight characters. Internally, this sets SecurityDomainType to the string cellQualified.

  All servers in the cell will prepend the security domain name you specify to the application-specific J2EE™ role name to create the SAF EJBROLE profile for checking. The security domain name is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.
The security domain name is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs that the Customization Dialog generates create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a security domain identifier, leave this field blank.

- **WebSphere Application Server unauthenticated user ID:**
  
  Associated with unauthenticated client requests. It is sometimes referred to as the “guest” user ID. It should be given the RESTRICTED attribute in RACF, to prevent it from inheriting UACC-based access privileges. The UNIX System Services UID number for the user ID is specified here and is associated with unauthenticated client requests. The UID value must be unique numeric values between 1 and 2,147,483,647.

- **Enable Writable SAF Keyring support**

  In previous versions of WebSphere Application Server, keystores and truststores that pointed to an SAF keyring could only be used in read only mode. Certificates stored in SAF could not be created, deleted, imported, or exported. These operations needed to be performed by the SAF administrator. In WebSphere V6.1, certificates stored in SAF could be viewed and their expirations could be monitored in the administrative console.

  With WebSphere Application Server for z/OS V7, the writable keyring support has been introduced. This feature enhances the capabilities of the administrative console to consistently manage keyrings and certificates stored in SAF. With the writable keyrings support, certificates can be created and signed by a CA, connected to keyrings, removed from keyrings, imported, exported and renewed using the administrative console. This major enhancement increases the efficiency of SSL management within WebSphere Application Server for z/OS while SAF still has control over all certificates and keyrings.

  All certificates created with the writable keyring support are generated and signed by Java™ code and not by SAF. In this case the writable keyring support only uses SAF to store the generated certificates.

  The writable keyring support is completely optional. New keystores and truststores marked as read-only can be created independent from the writable keyring support. When using the read-only JCERACFKS and JCECCARACFS keystores, the certificates in the appropriate SAF keyring can still be viewed in the administrative console.

  Click **Next**.
19. The next window (Figure 23) allows you to tailor the JCL for the customization jobs. Enter a valid job statement for your installation on this window. The profile creation process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

![Deployment manager: job statement definition](image)

Click **Next**.

20. The last window shows a short summary of the customization, including profile type and where the generated jobs will be stored. To change the characteristics of this profile, click the **Back** button; otherwise, click **Create** to generate your z/OS Customization jobs.

21. The PMT will display a summary window (Figure 24 on page 37) that indicates whether the jobs were created successfully or not. If the jobs were not created, a log file containing failure information will be identified.
The customization definition was successfully created.

Customization definition name:

WPDeploymentManager

The response file for this definition was written to:

C:\WAS V7\WAS WCT PMT\profiles\WPDeploymentManager\WPDeploymentManager.response

Note: Do not modify this response file, or subsequent actions on this customization definition might fail.

Click Finish to close this dialog and continue. Refer to the Customization Instructions view for the generated instructions, which explain the remaining steps that are needed to create the target WebSphere Application Server for z/OS runtime environment.

The information center contains additional information on running the z/OS customization jobs.

View the online information center

Figure 24  Deployment manager: Customization definition summary

Click Finish to return to the Profile Management Tool main panel. The new deployment manager definition will be listed in the Customization Definitions tab.
Uploading the jobs to the z/OS system

If successful, the next step in the z/OS customization process is to upload these jobs and the associated instructions to a pair of z/OS partitioned data sets. To do this,

1. On the main window, select the customization definition for the profile and click the **Process** button. To upload the generated jobs to the target z/OS system select **Upload to target z/OS system** and click **Next**.

2. In the upload customization definition window (Figure 25 on page 39), enter the target z/OS system. This must be fully qualified or the upload will fail.

   Use the **Allocate target z/OS data sets** check box to specify whether to allocate the data sets if they do not exist. If the data sets exist and are to be reused, clear the box.
Click **Finish**.

You can see a progress information window while the upload is occurring.
Executing the jobs

After the customization profile is uploaded, the next step is to execute the jobs. The instructions for preparing for and executing the jobs can be found in the Profile Management Tool. Select the customization definition and switch to the Customization Instructions tab (Figure 26). These instructions are also contained in a job that has been loaded to the host.

![Customization Definitions](image)

**WebSphere Application Server for z/OS customization instructions:**

Deployment manager WPDMGR (cell WPCELL, node WPDMNODE)
Tailored on 2009/05/05 at 13:14 by sadtler
WCT version 7.0.0.3 build cf030908.27

The Profile Management Tool has created a response file based on the information you provided. These instructions tell you how to convert this response file into a set of customization jobs and how to run the jobs to customize WebSphere Application Server for z/OS. When you upload the customization jobs to the target system, a text version of these instructions will be written to:

JVESER.WAS70.WPDMINODE.CNTL (BBOCCINS)
The instructions help you determine what jobs to run, the order to run them in, and the expected results. They also tell you how to start the environment after you are done.

After the jobs have been run successfully, the deployment manager profile is complete.

Figure 27 shows an example of the jobs generated to create a deployment manager and the sequence they should run in.

<table>
<thead>
<tr>
<th>The jobs and the sequence they’re run is very similar to before, with a few differences:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BBOCCINS</strong></td>
</tr>
<tr>
<td><strong>BBOSBRAK</strong></td>
</tr>
<tr>
<td><strong>BBODBRAK</strong></td>
</tr>
<tr>
<td><strong>BBOSBRAM</strong></td>
</tr>
<tr>
<td><strong>BBODCPY1</strong></td>
</tr>
<tr>
<td><strong>BBODCFS</strong></td>
</tr>
<tr>
<td><strong>BBODHFS</strong></td>
</tr>
<tr>
<td><strong>BBOWWPFD</strong></td>
</tr>
</tbody>
</table>

*Figure 27  Deployment manager configuration jobs created by PMT*
Figure 28 illustrates how the jobs are mapped to the components of the configuration.

### Mapping Jobs to the Three Basic Components of a Configuration

A configuration has three basic components -- a file system with configuration XML, JCL start procedures and SAF profiles.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daemon CR</td>
<td>Allocate/mount</td>
</tr>
<tr>
<td>DMGR CR</td>
<td></td>
</tr>
<tr>
<td>DMGR SR</td>
<td>SAF Profiles</td>
</tr>
<tr>
<td>LPAR A</td>
<td>SAF Profiles</td>
</tr>
<tr>
<td>/wasconfig/wpcell/wpdmnode</td>
<td>Copy procs</td>
</tr>
<tr>
<td>/DeploymentManager/profiles/default</td>
<td></td>
</tr>
<tr>
<td>/config</td>
<td>BBODZFS</td>
</tr>
<tr>
<td>/cells</td>
<td></td>
</tr>
<tr>
<td>/mycell</td>
<td>BBODHFSA</td>
</tr>
<tr>
<td>/nodes</td>
<td></td>
</tr>
<tr>
<td>/mydmnode</td>
<td>Create Directories</td>
</tr>
<tr>
<td>/servers</td>
<td>Copy in skeleton XML</td>
</tr>
<tr>
<td>/dmgr</td>
<td>Create customized profile</td>
</tr>
<tr>
<td>was.env</td>
<td></td>
</tr>
<tr>
<td>MYDCR</td>
<td>BBODCPY1</td>
</tr>
<tr>
<td>MYDSR</td>
<td></td>
</tr>
<tr>
<td>MYDEMN</td>
<td></td>
</tr>
<tr>
<td>SYS1.PROCLIB</td>
<td></td>
</tr>
</tbody>
</table>

Figure 28  Mapping generated jobs to configuration functions
Creating the base application server definition

The next step in building the sample environment is to create a standalone application server.

To begin, run the profile management tool to create the customization definition:

1. Click **Create** on the Profile Management Tool main panel.
   - The first panel that you see when you click **Next** on the Profile Management Tool Welcome panel prompts you to select the type of WebSphere environment that you want to create.

2. In the environment selection panel, select **Application server** as shown in Figure 29 and click **Next**.

3. Specify a name for the customization definition and optionally a response file path, and click **Next**.

![Figure 29 Selecting Application server environment](image_url)
4. The next panel (Figure 30) lets you establish configuration default values.

![Profile Management Tool 7.0 Default Values](image)

**Figure 30** Application server default values

The GID and UID defaults section contains the following selectable option:

- **Set each default GID and UID value to indicate that operating-system security is to assign an unused value:**

  When this option is selected, each GID and UID value is defaulted to allow operating-system security to assign an unused value. When this option is not selected, each GID and UID value is defaulted to an IBM-provided number.

**Note:** If you specified a response file for setting default values, any default selected here will override the corresponding response file values.
The Name and user ID defaults contain the following selectable options:

- **Set default names and user IDs based on cell, cluster, and system identifiers:**

  When this option is selected, default cell, node, server, cluster, and procedure names as well as group names and user IDs are based on cell, cluster, and system identifiers.

- **Application server will be federated into a Network Deployment cell:**

  Select this option to indicate that the application server will be federated into a Network Deployment cell at some point in time.

- **Two-character cell identifier:**

  Enter a two-character cell identifier to be used to create default names and user IDs.

  If you have selected the option to federate to a cell, specify the two-character cell identifier of the target Network Deployment cell.

  **Rule:** The first character must be an alphabetic character and the second character must be an alphanumeric character. Alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

- **Two-character cluster identifier:**

  Two-character cluster identifier to be used to create default names and user IDs. The characters will be appended to the cluster transition name.

  **Rule:** The characters must be alphabetic characters. The alphabetic characters can be entered in lowercase or uppercase. The case of alphabetic characters will be adjusted as appropriate for each generated default value.

- **Single-character system identifier:**

  Single-character system identifier to be used to create default names and user IDs. It will be appended to the short and long names for the cell, node, and server and to the appropriate process names.

  **Rule:** The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.
– Port defaults:
  Select default port values from the following port range.
  When this option is not selected, each port value defaults to an IBM-provided number. When this option is selected, each port default value is selected from the following port number range.
  The port range must contain at least 20 ports.
– Lowest default port number:
  Lowest number that can be assigned as a default port number
– Highest default port number:
  Highest number that can be assigned as a default port number
Click **Next**.

5. You are now prompted to specify the high-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions that are being created. (See Figure 11 on page 16).

The generated batch jobs and instructions will be uploaded to two z/OS partitioned datasets:

– *HLQ.CNTL*
  Partitioned dataset with fixed block 80-byte records to contain customization jobs

– *HLQ.DATA*
  Partitioned dataset with variable-length data to contain other data contained in the customization definition

**Note:** A multilevel high-level qualifier can be specified as the dataset high-level qualifier

Click **Next**.
6. The Configure Common Groups panel appears as shown in Figure 31.
– WebSphere Application Server configuration group information:
  Specify the default group name for the WebSphere Application Server administrator user ID and all server user IDs.
  Select whether to allow the OS security system (RACF) to assign an unused GID value, or assign a specific GID.

– WebSphere Application Server servant group information:
  Specify the group name for all servant user IDs. You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.
  Select whether to allow the OS security system (RACF) to assign an unused GID value, or assign a specific GID.

– WebSphere Application Server local user group information:
  Specify the group name for local clients and unauthorized user IDs (provides minimal access to the cell).
  Select whether to allow the OS security system (RACF) to assign an unused GID value, or assign a specific GID.

**GID values:** The specified GID is the UNIX System Services GID number for the WebSphere Application Server configuration group. GID values must be unique numeric values between 1 and 2,147,483,647.

Click **Next**.

7. The Configure Common Users panel appears as shown in Figure 32 on page 49.
Figure 32 Configure Common Users
– Common controller user ID:

**UIDs:** UIDs must be unique numbers between 1 and 2,147,483,647 within the system.

Enter the user ID to be associated with all the control regions and the daemon. This user ID will also own all of the configuration file systems. If you are using a non-IBM security system, the user ID might have to match the procedure name. Refer to your security system's documentation.

Select whether to allow the OS security system (RACF) to assign an unused UID value, or assign a specific UID to be associated with the control region user ID.

– Common servant user ID:

Enter the user ID to be associated with the servant and control adjunct regions.

Select whether to allow the OS security system (RACF) to assign an unused UID value, or assign a specific UID to be associated with the servant region user ID.

– WebSphere Application Server administrator:

Enter the user ID for the initial WebSphere Application Server administrator. The user ID must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Select whether to allow the OS security system (RACF) to assign an unused UID value, or assign a specific UID to be associated with the administrator user ID.

– Asynchronous administration user ID:

Enter the user ID to be used to run asynchronous administration operations procedure. This ID must be a member of the WebSphere Application Server configuration group.

Select whether to allow the OS security system (RACF) to assign an unused UID value, or assign a specific UID for the asynchronous administration task user ID.

– WebSphere Application Server user ID home directory:

This field identifies a new or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process. This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

Click **Next**.
8. Provide the system and data set names to be used (See Figure 14 on page 21):
   – Specify the system and sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS.
   – Enter the name of an existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added.

   Click **Next**.

9. Next the Cell, Node, and Server names panel is presented as shown in Figure 33 on page 52.
   – Specify the long and short names for the cell, node, and servers. Short names identify the process to z/OS facilities, such as SAF. Long names are used as the primary external identification for the process. This is the name you will see in the administrative console.
   – Cluster transition name:
     If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster.
   – Specify the JVM™ mode. With Version 7.0 either 31 bit or 64 bit can be selected. The default value is 64 bit, because the 31 bit has been deprecated.

   Click **Next**.
Figure 33  Cell, Node, and Server Names
Figure 34  Configuration file system settings
10. The Configuration File System values are entered as shown in Figure 35 on page 55:

- Mount point:
  Application server configuration file system mount point: Specifies the Read/write file system directory where the application data and environment files are written. This field is not writable here, but was specified earlier on the "System Environment: Configuration file system information" window.

- Directory path name relative to mount point:
  The relative path name of the directory within the configuration file system in which the application server configuration resides.

- Data set name:
  The file system data set you will create and mount at the specified mount point above.

- Volume, or '*' for SMS:
  Specify either the DASD volume serial number to contain the above data set or '*' to let SMS select a volume. Using '*' requires that SMS automatic class selection (ACS) routines be in place to select the volume. If you do not have SMS set up to handle data set allocation automatically, list the volume explicitly.

- Primary allocation in cylinders:
  The initial size allocation for the configuration file system data set. In the application server, the total space needed for this data set increases with the size and number of the installed applications. The minimum suggested size is 250 cylinders (3390).

- Secondary allocation in cylinders:
  The size of each secondary extent. The minimum suggested size is 100 cylinders.

- File System type:
  Select to allocate and mount your configuration file system data set using HFS or zFS.
11. Specify the information for the product file system as shown in Figure 35.

![Profile Management Tool 7.0](image)

- Specify the name of the directory where the product files for WebSphere Application Server for z/OS were stored during installation.
- Select the option to allow to set up an intermediate symbolic link and specify the path name.

Click **Next**.
12. The next panel allows you to select the applications to deploy onto the environment that you are creating. The choices are:

- Administrative console (recommended)
- Default application
- Sample applications

Click **Next**.

13. Enter the process information into the panel shown in Figure 36. The job names for the processes are provided in the panel and cannot be changed. Specify the procedure name for each process.

![Figure 36 Application server names](image-url)
– Controller process job and procedure name:
The job name for the control region is the same as the server short name. This is the name used in the MVS START command to start the region.

– Controller adjunct process job and procedure name:
The job name is used by WLM to start the control region adjunct. This is set to the server short name followed by the letter “A.”

– Servant process job and procedure name:
The job name is used by WLM to start the servant regions. This is set to the server short name followed by the letter “S.”

– Admin asynch operations procedure name:
Specify the JCL procedure name of a started task to be launched by way of the START command by node agents or application servers to perform certain asynchronous administrative operations (such as node synchronization) and add and remove a node.

Click Next.

14. Specify the application server port values into the panel shown in Figure 37 on page 58.

Good planning is very important to avoid port conflicts, so be sure that you have all values you need in order to fill out this panel.
Click **Next**.
Location Service Daemon Definitions are shown in Figure 38.

- Daemon home directory: Directory in which the location service daemon resides. This is set to the configuration file system mount point/Daemon and cannot be changed.
- Daemon job name: Specifies the job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon.
- Procedure name: Name of the member in your procedure library to start the location service daemon.
- IP Name: The fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses.
- Listen IP: Address at which the daemon listens.
- Port: Port number on which the location service daemon listens.
- SSL port: Port number on which the location service daemon listens for SSL connections.
- Register daemon with WLM DNS: If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it; otherwise, do not select it.

Click **Next**.

16. Next the SSL Customization panel is presented. This is similar to the deployment manager panel shown previously in Figure 21 on page 31. Enter the information required for SSL connections and click **Next**.

17. The next panel allows you to select the user registry that will be used to manage user identities and authorization policy. You can select from one of the following choices:

**Note:** If you plan to federate this application server, we recommend that you set the application server’s SAF profile prefix to be the same as that of the Network Deployment Cell.

- **z/OS security product option:** This option uses the z/OS system's SAF compliant security product, such as IBM RACF or equivalent, to manage WebSphere Application Server identities and authorization according to the following rules:
  - The SAF security database will be used as the WebSphere user repository.
  - SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
  - Digital certificates will be stored in the SAF security database.

**Note:** Select the z/OS security product option if you are planning to use the SAF security database as your WebSphere Application Server registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking. For this security option, you must decide whether to set a security domain name, and choose an administrator user ID and an unauthenticated (guest) user ID.
- WebSphere Application Server security option: The WebSphere Application Server administrative security option is used to manage the Application Server identities and authorization as follows:
  - A simple file-based user registry will be built as part of the customization process.
  - Application-specific role binds will be used to control role-based authorization.
  - The WebSphere Application Server console users and groups list will control administrative authority.
  - Digital certificates will be stored in the configuration file system as keystores.

  **Note:** Choose this option if you plan to use an LDAP or custom user registry without mapping to SAF user IDs. (The file-based user registry is not recommended for production use.)

- No security:
  Although it is not recommended, you can disable administrative security. If you choose this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually. You can enable security manually later via the administrative console or using Jython scripts.

  Select an option and click **Next**. The next window you see will depend on the security option you choose.

18. The next panel displayed will depend on the Security option you selected. We previously selected the **Use a z/OS security product** option and were presented with the panel shown in Figure 39 on page 62.
SAF profile prefix: (Formally known as Security domain identifier):

This optional parameter is used to distinguish between APPL or EJBROLE profiles based on security domain name. It provides an alphanumeric security domain name of one to eight characters. Internally, this sets SecurityDomainType to the string cellQualified.
All servers in the cell will prepend the security domain name you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking. The security domain name is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The security domain name is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs that the Customization Dialog generates create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a security domain identifier, leave this field blank.

- **WebSphere Application Server unauthenticated user ID:**
  Associated with unauthenticated client requests. It is sometimes referred to as the “guest” user ID. It should be given the RESTRICTED attribute in RACF, to prevent it from inheriting UACC-based access privileges. The UNIX System Services UID number for the user ID is specified here and is associated with unauthenticated client requests. The UID value must be unique numeric values between 1 and 2,147,483,647.

- **Enable Writable SAF Keyring support**
  In previous versions of WebSphere Application Server keystores and truststores that pointed to a SAF keyring could only be used in read only mode. Certificates stored in SAF could not be created, deleted, imported or exported. These operations needed to be performed by the SAF administrator. In WebSphere V6.1, certificates stored in SAF could be viewed and their expirations could be monitored in the administrative console.

  With WebSphere Application Server for z/OS V7 the writable keyring support has been introduced. This feature enhances the capabilities of the administrative console to consistently manage keyrings and certificates stored in SAF.

  With the writable keyrings support, certificates can be created and signed by a CA, connected to keyrings, removed from keyrings, imported, exported and renewed using the administrative console. This major enhancement increases the efficiency of SSL management within WebSphere Application Server for z/OS while SAF still has control over all certificates and keyrings.

  All certificates created with the writable keyring support are generated and signed by Java code and not by SAF. In this case the writable keyring support only uses SAF to store the generated certificates.
The writable keyring support is completely optional. New keystores and truststores marked as read-only can be created independent from the writable keyring support. When using the read-only JCERACFKS and JCECCARACFS keystores, the certificates in the appropriate SAF keyring can still be viewed in the administrative console.

Click **Next**.

19. The next panel allows you to customize the JCL for the generated jobs. The panel is the same as seen in the deployment manager scenario (Figure 23 on page 36.)

Make any adjustments necessary and click **Next**.

20. The Customization Summary is the final panel presented. Click **Create** to store this application server environment definition for later transfer to the intended z/OS host system.

21. Click **Finish** when the jobs are complete.

If successful, the next step in the z/OS customization process is to upload these jobs and the associated instructions to a pair of z/OS partitioned data sets. To do this,

1. On the main window, select the customization definition for the profile and click the **Process** button. To upload the generated jobs to the target z/OS system select **Upload to target z/OS system** and click **Next**.

2. In the upload customization definition window (Figure 25 on page 39), enter the target z/OS system. This must be fully qualified or the upload will fail.

   Use the **Allocate target z/OS data sets** check box to specify whether to allocate the data sets if they do not exist (box check). If the data sets exist and are to be reused, clear the box.

   Click **Finish**.

   You will see a progress information window while the upload is occurring.

3. After the customization profile is uploaded, select the customization definition in the Profile Management Tool and switch to the **Customization Instructions** tab. This will provide you with complete instructions on how to build the profile using the jobs.

   These instructions will help you determine what jobs to run, the order to run them in, and the expected results. It will also tell you how to start the environment after you are done.

   After the jobs have been run successfully, the application server profile is complete.
Federating an application server

This definition is used to federate the base application server into the previously created deployment manager node:

1. Select **Federate an application server** in the Environment Selection panel as shown in Figure 40.

![Figure 40 Federate an application server selection](image)

Click **Next**.

2. Enter a name for the customization definition and click **Next**.

3. The Default Values panel next appears as shown in Figure 41 on page 66.
Figure 41  Default port settings

This panel allows you to specify a default range of ports to be used for the node agent. When this option is not selected, each port value defaults to an IBM-provided number.

Click **Next**.

4. The Target Data Sets panel allows you to provide the high-level qualifier for the pair of data sets (CNTL and DATA) that will contain the generated jobs. (See Figure 11 on page 16).

Click **Next**.
5. The Federate Application Server (Part 1) panel appears as shown in Figure 42. This panel is used to specify the information needed to access the application server and the deployment manager.

Figure 42 Specify Application server settings (Part 1)
– Application server access information:

This section contains the information needed to find and access the application server node configuration file system. This information includes the file system mount point, the directory path name, and if administrative security is enabled on the application server, the administrator user ID and password.

– Deployment manager access information:

Federating the application server requires that the deployment manager be running and accessible by the federation process. This section provides the information required to connect to the deployment manager, including the host name or IP address, JMX™ connection type and port, and the administrator user ID and password.

The node host name must always resolve to an IP stack on the system where the deployment manager runs. The node host name cannot be a DVIPA or a DNS name that, in any other way, causes the direction of requests to more than one system.

The user ID and password are required when global security is enabled on the Network Deployment cell unless an RMI connector is being used. If an RMI connector is being used, the identity information will be extracted from the thread of execution of the addNode job if the user ID and password are not specified.

Click Next.

6. The next panel is shown in Figure 43 on page 69. The output of this panel is used to configure the node agent required for the application server to participate in the distributed environment cell.
Figure 43  Specify Application server settings (Part 2)
– Specify the short name for the node agent process:
   The short name is the server's jobname, as specified in the MVS START command JOBNAME parameter. (The node agent server long name is set to the fixed value of nodeagent.)
– Specify the IP addresses and ports to be used by the node agent and a new ORB port to be used by the application server.
– The node group, configuration group, and configuration user ID.
– Select the relevant federation options for your environment. If you have installed applications on the application server or defined service integration buses, you can choose to have those included in the newly federated application server.

Click Next.

7. The Job Statement Definition panel is displayed next (see Figure 23 on page 36). All the customization jobs that will be created will need a job statement. Enter a valid job statement for your installation and click Next.

8. Finally, a summary is displayed. Click Create, then Finish.

If successful, the next step in the z/OS customization process is to upload these jobs and the associated instructions to a pair of z/OS partitioned data sets. To do this:

1. On the main window, select the customization definition for the profile and click the Process button. To upload the generated jobs to the target z/OS system, select Upload to target z/OS system and click Next.

2. In the upload customization definition window (Figure 25 on page 39), enter the target z/OS system. This must be fully qualified or the upload will fail.

   Use the Allocate target z/OS data sets check box to specify whether to allocate the data sets if they do not exist (check box). If the data sets exist and are to be reused, clear the box.

   Click Finish.

   You will see a progress information window while the upload is occurring.

3. After the customization profile is uploaded, select the customization definition in the Profile Management Tool and switch to the Customization Instructions tab. This provides you with complete instructions on how to build the profile using the jobs.

   These instructions can help you determine what jobs to run, the order to run them in, and the expected results. It also tells you how to start the environment after you are done.

   After the jobs have been run successfully, the application server profile is complete.
Creating a job manager profile

In a flexible management environment, the job manager allows you to asynchronously submit and administer jobs for large numbers of unfederated application servers and deployment managers over a geographically dispersed area. Many of the management tasks that you can perform with the job manager are tasks that you can already perform with the product, such as application management, server management, and node management. However, with the job manager, you can aggregate the tasks and perform the tasks across multiple application servers or deployment managers.

The next panel prompts you to select the type of WebSphere environment that you want to create:

1. To generate the definitions for the Job Manager select Management in the PMT environment selection panel and click Next.
2. In the next panel, select Job manager as the type and click Next.
3. Specify a name for the customization definition and click Next.
4. The next panel allows you to specify defaults for GID and UID values, name and user ID defaults based on a two character prefix that identifies the cell, and allows you to specify a default range for ports assigned to the process. Click Next.
5. The next panel allows you to specify the high level qualifier for the CNTL and DATA data sets that will hold the generated jobs and instructions (see Figure 11 on page 16). Specify the value and click Next.
6. The next panel (Figure 44) allows you to configure the common groups.

![Figure 44](image.jpg)

**Figure 44**  Job Manager: Common group settings

Provide the appropriate settings for your environment into the common groups panel and click **Next**.
7. Next, configure the user ID settings (Figure 45).

Figure 45   Job Manager: Common Users settings
Provide the appropriate settings for your environment and click **Next**.

8. Enter the required information into the System and Data Set Names panel as shown in Figure 14 on page 21. Click **Next**.

9. Enter the cell, node, and server names to use for this profile into the panel shown in Figure 46.

**Note:** Each management server (administrative agent, deployment manager, or job manager) should be assigned its own cell name that is different from that of any other WebSphere Application Server cell on the same z/OS sysplex.

![Figure 46 Job Manager: cell, node and server names](image-url)
Click **Next**.

10. Enter the file system information to be used for the job manager configuration data as shown in Figure 47 and click **Next**.

![Figure 47 Job Manager: file system settings](image)
11. Enter the product file system information for the job manager as shown in Figure 48 similarly to what was described for the Application Server environment shown in Figure 35 on page 55. Click Next.

![Profile Management Tool 7.0]

Figure 48   Job Manager: product file system location
12. Enter the procedure names to be used for the job manager controller process and server process as shown in Figure 49. Click **Next**.
13. Enter the job manager port values as shown in Figure 50. Click **Next**.

![Port Values Assignment](image)

**Figure 50  Job manager port values**
14. Enter the appropriate values into the Location Service Daemon Definitions panel as shown in Figure 51. Click **Next**.

![Figure 51 Job manager: Location Service Daemon settings](image)

15. The SSL Customization panel is presented next. Enter the information required for SSL connection. (see Figure 21 on page 31). Click **Next**.

16. The next panel allows you to select the user registry. Select from one of the following choices:
- Use a z/OS security product
- Use WebSphere Application Server
- Do not enable security
Click **Next**. The next panel you see will depend on the user registry option you select.

17. In this example, the **z/OS security product** user registry option was selected in the previous step. The next panel allows you to configure parameters specific to this option (Figure 52).

![Job manager: Security settings](image)

**Figure 52  Job manager: Security settings**

Click **Next**.

18. The next panel allows you to modify the JCL to be used in the generated jobs. Modify the JCL or accept the defaults and click **Next**.

19. The last panel is a summary. Click **Create**, then **Finish** to store this Job manager environment definition for later transfer to the intended z/OS host system.

If successful, the next step in the z/OS customization process is to upload these jobs and the associated instructions to a pair of z/OS partitioned data sets.
To do this:

1. On the main window, select the customization definition for the profile and click the **Process** button. To upload the generated jobs to the target z/OS system select **Upload to target z/OS system** and click **Next**.

2. In the upload customization definition window (Figure 25 on page 39), enter the target z/OS system. This must be fully qualified or the upload will fail.

   Use the **Allocate target z/OS data sets** check box to specify whether to allocate the data sets if they do not exist (box check). If the data sets exist and are to be reused, clear the box.

   Click **Finish**.

   You will see a progress information window while the upload is occurring.

3. After the customization profile is uploaded, select the customization definition in the Profile Management Tool and switch to the **Customization Instructions** tab. This will provide you with complete instructions on how to build the profile using the jobs.

   These instructions will help you determine what jobs to run, the order to run them in, and the expected results. It will also tell you how to start the environment after you are done.

   After the jobs have been run successfully, the application server profile is complete.

---

**Creating an administrative agent profile**

The administrative agent provides a single interface to administer multiple application server nodes in, development, unit test, or server farm environments, for example. The administrative agent provides a single interface to administer multiple unfederated application server nodes in, for example, development, unit test, or server farm environments. By using a single interface to administer your application servers, you reduce the overhead of running administrative services in every application server.

1. To generate the definitions for the administration agent select **Management** in the PMT environment selection panel and click **Next**.

2. Select **Administrative agent** as the server type and click **Next**.

3. Enter a name for the customization definition and click **Next**.

4. The next panel allows you to specify defaults for GID and UID values, name and user ID defaults based on a two character prefix that identifies the cell, and allows you to specify a default range for ports assigned to the process.
Click **Next**.

5. The next panel allows you to specify the high level qualifier for the CNTL and DATA data sets that will hold the generated jobs and instructions (see Figure 11 on page 16). Specify the value and click **Next**.

6. Configure the common group settings as shown in Figure 53.
Provide the appropriate settings for your environment and click Next.

7. Configure the common user settings as shown in Figure 54.

![Configuration interface for common users](image.png)

**Figure 54** Administrative agent: common users
Provide the appropriate settings for your environment and click **Next**.

8. Next enter the system name, sysplex name, and PROCLIB data set name (See Figure 14 on page 21). Click **Next**.

9. Enter the cell, node, and server names as shown in Figure 55 and click **Next**.

![Figure 55  Cell, node and server names](image-url)
10. Enter the file system information for the administrative agent as shown in Figure 56.

![Figure 56: Configuration file system settings](image-url)

**Figure 56** Configuration file system settings
11. Enter the product file system information for the administrative agent as shown in Figure 57 and click **Next**.

*Figure 57  Administrative agent: product file system*
12. Enter the job manager controller process and server process names as shown in Figure 58 and click **Next**.

![Profile Management Tool 7.0](image)

**Figure 58  Controller and servant names**
13. Enter the administrative agent port values similar to those shown in Figure 59 and click **Next**.

*Figure 59  Administrative agent: port assignments*
14. Enter the appropriate values into the Location Service Daemon Definitions panel as shown in Figure 60 and click **Next**.

![Figure 60 Location service daemon settings](image)

15. The SSL Customization panel is presented next. Enter the information required for SSL connection. (see Figure 21 on page 31). Click **Next**.

16. The next panel allows you to select the user registry. Select from one of the following choices:
   - Use a z/OS security product
   - Use WebSphere Application Server
   - Do not enable security
Click **Next**. The next panel you see will depend on the user registry option you select.

17. In this example, the **z/OS security product** user registry option was selected in the previous step. The next panel allows you to configure parameters specific to this option (Figure 61).

![Figure 61  Administration agent security settings](image)

18. The next panel allows you to modify the JCL to be used in the generated jobs. Modify the JCL or accept the defaults and click **Next**.

19. The last panel is a summary. Click **Create**, then **Finish** to store this Job manager environment definition for later transfer to the intended z/OS host system.

If successful, the next step in the z/OS customization process is to upload these jobs and the associated instructions to a pair of z/OS partitioned data sets.
To do this:

1. On the main window, select the customization definition for the profile and click the **Process** button. To upload the generated jobs to the target z/OS system select **Upload to target z/OS system** and click **Next**.

2. In the upload customization definition window (Figure 25 on page 39), enter the target z/OS system. This must be fully qualified or the upload will fail.
   
   Use the **Allocate target z/OS data sets** check box to specify whether to allocate the data sets if they do not exist (check box). If the data sets exist and are to be reused, clear the box.

   Click **Finish**.

   You will see a progress information window while the upload is occurring.

3. After the customization profile is uploaded, select the customization definition in the Profile Management Tool and switch to the **Customization Instructions** tab. This will provide you with complete instructions on how to build the profile using the jobs.

   These instructions will help you determine what jobs to run, the order to run them in, and the expected results. It will also tell you how to start the environment after you are done.

   After the jobs have been run successfully, the application server profile is complete.

   After the administrative agent and standalone application servers have been created on the system, use the **registerNode** command to register the application server nodes to the administrative agent.
Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:
This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM’s application programming interfaces.

© Copyright International Business Machines Corporation 2009. All rights reserved.
Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
This document REDP-4571-00 was created or updated on October 13, 2009.

Send us your comments in one of the following ways:
- Use the online Contact us review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an email to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099, 2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

- DataPower®
- DB2®
- IBM®
- RACF®
- Redbooks (logo)®
- WebSphere®
- z/OS®

The following terms are trademarks of other companies:

- ACS, and the Shadowman logo are trademarks or registered trademarks of Red Hat, Inc. in the U.S. and other countries.
- J2EE, Java, JMX, JVM, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.