Chapter 2 of *WebSphere Application Server V7 Administration and Configuration Guide,* SG24-7615

WebSphere Application Server V7: Working with Profiles on Distributed Systems

Installing a WebSphere Application Server environment requires careful planning. A major decision point is the topology for the system. These decisions include, for example, whether you will have a standalone server, a distributed managed server environment, and whether you will use the new flexible management options.

Planning for topology design is covered in the IBM® Redbooks® publication *WebSphere Application Server V7: Concepts, Planning and Design*, SG24-7708. That book is designed to help you select a topology and develop a clear idea of what steps are needed to set up your chosen environment. Your options depend on your WebSphere® Application Server package. The installation process is well-documented in the installation guide packaged with the product. The purpose of this chapter is to help you build your initial WebSphere Application Server environment after you have installed the product. We cover the following topics:

Types of profiles

The WebSphere Application Server installation process simply lays down a set of core product files required for the runtime processes. After installation, you need to create one or more *profiles* that define the runtime to have a functional system. The core product files are shared among the runtime components defined by these profiles.

With the Base and Express packages, you can only have standalone application servers. Each application server is defined within a single cell and node. The administration console is hosted within the application server and can only connect to that application server. ***(New in V7)*** You can consolidate administration for multiple standalone servers by registering the node for each application server to an administrative agent.

The application server profile defines the standalone environment. You can also create standalone application servers with the Network Deployment package, although you will most likely do so with the intent of federating that server into a cell for central management.

With the Network Deployment package, you have the option of defining multiple application servers with central management capabilities. The administration domain is the cell, consisting of one or more nodes. Each node contains one or more application servers and a node agent that provides an administration point management by the deployment manager.

The deployment manager can be located on the same machine as one or more of the application servers—a common topology for single machine development and testing environments. In most production topologies, we recommend that the deployment manager be placed on a separate dedicated machine.

The basis for this runtime environment starts with the deployment manager that provides the administration interface for the cell. As you would expect, the deployment manager is defined by a deployment manager profile.

Nodes can be added to the cell in one of two ways:

- You can create an application server profile, then federate it to the cell. When a node is added to a cell, a node agent is created on the node, and configuration files for the node are added to the master configuration repository for the cell. The deployment manager then assumes responsibility for the configuration of all servers on the node.
- You can define a custom profile to create an empty node for federation to the cell. After federation, you further configure the node by creating application servers and clusters from the deployment manager administrative console.

With WebSphere Application Server V7.0, the job manager and administrative agent profile types have been introduced to enhance the administration capabilities.

Application server profile

The application server profile defines a single standalone application server. Using this profile gives you an application server that can run standalone, or unmanaged. The environment has the following characteristics:

- The profile consists of one cell, one node, and one server. The cell and node are not relevant in terms of administration, but you see them when you administer the server through the administrative console scopes.
- The application samples are installed on the server (optional).
- The server has a dedicated administrative console.

The following three examples are the primary uses for this type of profile:

- To build a standalone server in a Base or Express installation.
- To build a standalone server in a Network Deployment installation that is not managed by the deployment manager (a test machine, for example).
- To build a server in a distributed server environment to be federated and managed by the deployment manager. If you are new to WebSphere Application Server and want a quick way of getting an application server complete with samples, this is a good option. When you federate this node, the default cell becomes obsolete, the node is added to the deployment manager cell, and the administrative console is removed from the application server.

Deployment manager profile

The deployment manager profile defines a deployment manager in a distributed server environment. Although you can conceivably have the Network Deployment package and run only standalone servers, this approach bypasses the primary advantages of Network Deployment, which is workload management, failover, and central administration.

In a Network Deployment environment, you should create one deployment manager profile for each cell. This gives you:

- A cell for the administrative domain
- A node for the deployment manager
- A deployment manager with an administrative console
- No application servers

After you have the deployment manager, you can:

- Federate nodes built either from existing application server profiles or custom profiles.
- Create new application servers and clusters on the nodes from the administrative console.

Custom profile

A *custom profile* is an empty node, intended for federation to a deployment manager. This type of profile is used when you build a distributed server environment. You use a custom profile for these purposes:

1. Create a deployment manager profile.
2. Create one custom profile on each node on which you will run application servers.
3. Federate each custom profile to the deployment manager, either during the custom profile creation process or later by using the **addNode** command.
4. Create new application servers and clusters on the nodes from the administrative console.

Cell profile

A *cell profile* is actually a combination of two profiles: a deployment manager profile and an application server profile. The application server profile is federated to the cell. The deployment manager and application server reside on the same system. This type of profile lets you get a quick start with a distributed server environment and is especially useful for test environments that typically have all nodes on one test system.

Administrative agent profile

(New in V7) The *administrative agent* is a new profile that provides enhanced management capabilities for standalone application servers. This profile is a new concept introduced with WebSphere Application Server V7.0.

An administrative agent profile is created on the same node as the standalone servers and can only manage nodes on that server. The node configuration for each standalone server is totally separate from any other servers on the system, but it can be managed using the administrative console on the administrative agent.

To participate in flexible management, standalone base servers first register themselves with the administrative agent. When a base application server registers with an administrative agent, much of the administrative code that was in the base server is consumed by the administrative agent. This results in a significantly smaller and faster starting base server (Figure 1).

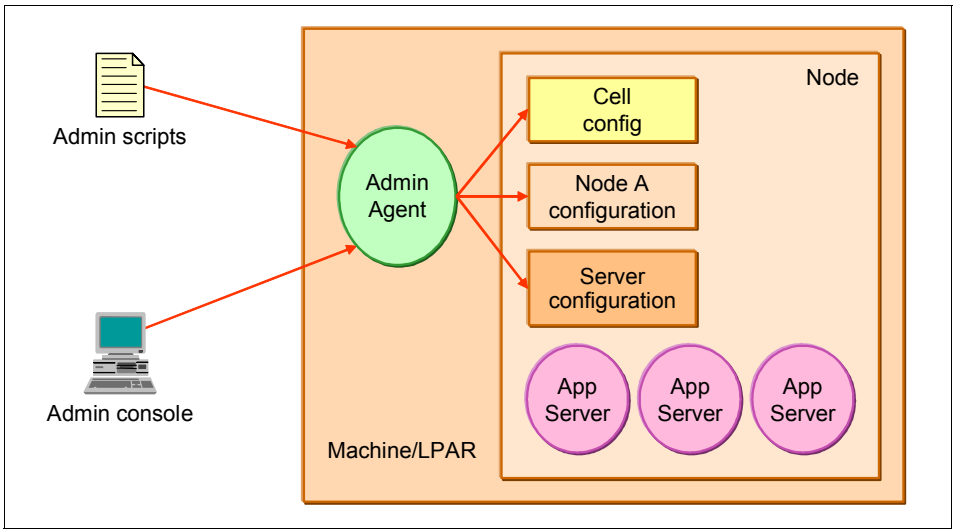

Figure 1 High-level overview of an administrative agent profile architecture

Job manager profile

(New in V7) The job manager is a new server type that was added to support flexible management. A job manager is defined by a job manager profile.

To participate in flexible management, a standalone application server first registers itself with the administrative agent. The administrative agent must then register the node for the application server with the job manager. If a deployment manager wants to participate in an environment controlled by a job manager, the deployment manager registers directly with the job manager; no administrative agent is involved in this case.

The main use of the job manager is to queue jobs to application servers in a flexible management environment. These queued jobs are pulled from the job manager by the administrative agent and distributed to the appropriate application server or servers.

Both deployment manager and administrative agents retain autonomy and can be managed without the job manager.

The units of work that are handled by the flexible management environment are known as *jobs*. The semantics of these jobs are typically straightforward, and the jobs require few parameters. The jobs are processed asynchronously and can have an activation time, expiration time, and a recurrence indicator. You can specify that an e-mail notification be sent upon completion of a job. Additionally, you can view the current status of a job by issuing a status command (Figure 2).

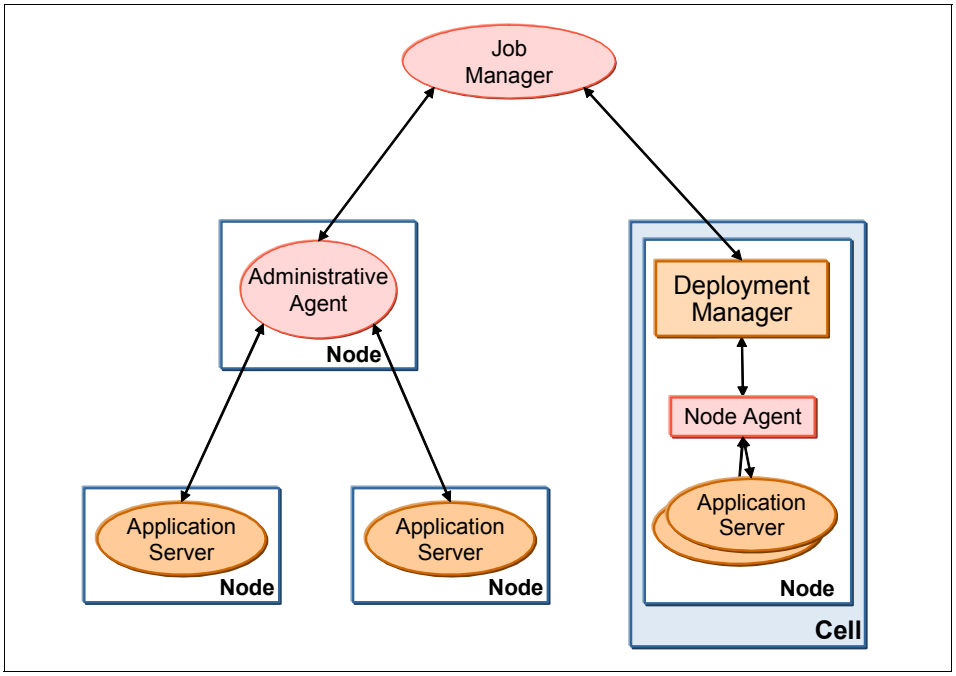

Figure 2 High-level overview of a job manager architecture

In Figure 2, we see that the administrative agent looks like it communicates directly to the job manager node - in practice the individual application server that is managed by the administrative agent is registered with the job manager directly.

Profile generation

Profiles can be created at any point of time during or after installation by using graphical or command line tools. The profile management tools provided with WebSphere Application Server are:

- The **`manageprofiles`** command: Command line interface for profile management functions.

- Profile Management Tool (PMT): A GUI interface that gathers user input and invokes the manageprofiles command line tool to manage the profiles.

Planning for profiles

Profiles can be created using the PMT or in silent mode using the **manageprofiles** command. Regardless of the method you use, a minimum amount of space must be available in the directory where you create a profile. This minimum requirement is documented in the Information Center at this Web site:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/rpro_diskspace.html

Profiles grow when applications and associated log files are created, and therefore, these increases must be considered at the planning stages.

An error can occur when you do not provide enough space to create a profile. Verify that you have, in addition to the minimum space required for a particular profile, an additional 40 MB of space, which is used for log files and temporary files.

Important: You cannot use the PMT to create profiles for WebSphere Application Server 64-bit installations except on the Linux® for zSeries® platform. However, you can use the Profile Management Tool on 64-bit architectures if you use a WebSphere Application Server 32-bit installation.

Building systems with profiles

This section shows how to use the PMT to create profiles on distributed systems. Creating profiles in silent mode is discussed in “Creating a profile with the manageprofiles command” on page 65.

Starting the PMT

The first steps in creating a profile are common, regardless of the type of profile you are going to create.

Follow these steps to create the profile:

1. Start the PMT using one of the following methods:
   - Windows® only:

     From the Start menu, select **Start** → **Programs** → **IBM WebSphere** → **Application Server Network Deployment V7.0** → **Profile Management Tool**.
   - For Linux, HP-UX, Solaris™, and AIX®:

     Use the **pmt.sh** command in the *install_root*/bin/ProfileManagement directory.
   - At the end of the installation process using the install wizard, check the box to launch the Profile Management Tool.
2. When you start the wizard, the first window you see is the Welcome window. Click the **Launch Profile Management Tool** button (Figure 3).

Figure 3 PMT Welcome window

3. Next, you see a list of existing profiles. Click **Create** to start the profile creation process (Figure 4).

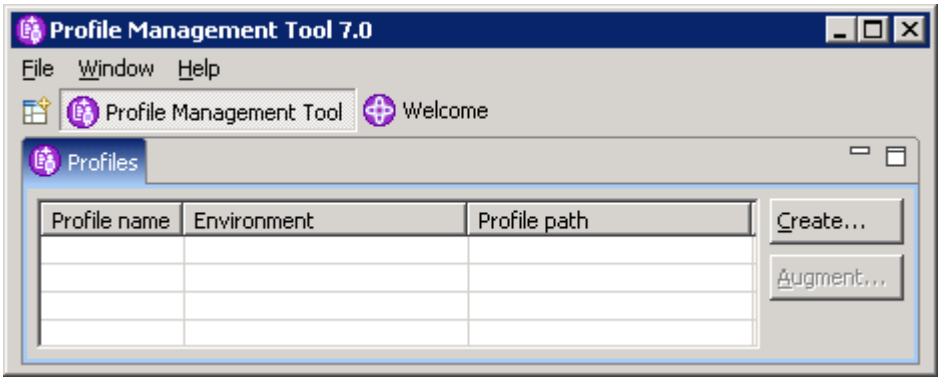

Figure 4 PMT List of profiles

Common panels and steps for all profiles

Many of the options that you have when you create a profile are the same, regardless of the type of profile.

Environment selection

During profile creation, you will be asked to select the type of profile to create (Figure 5 on page 10).

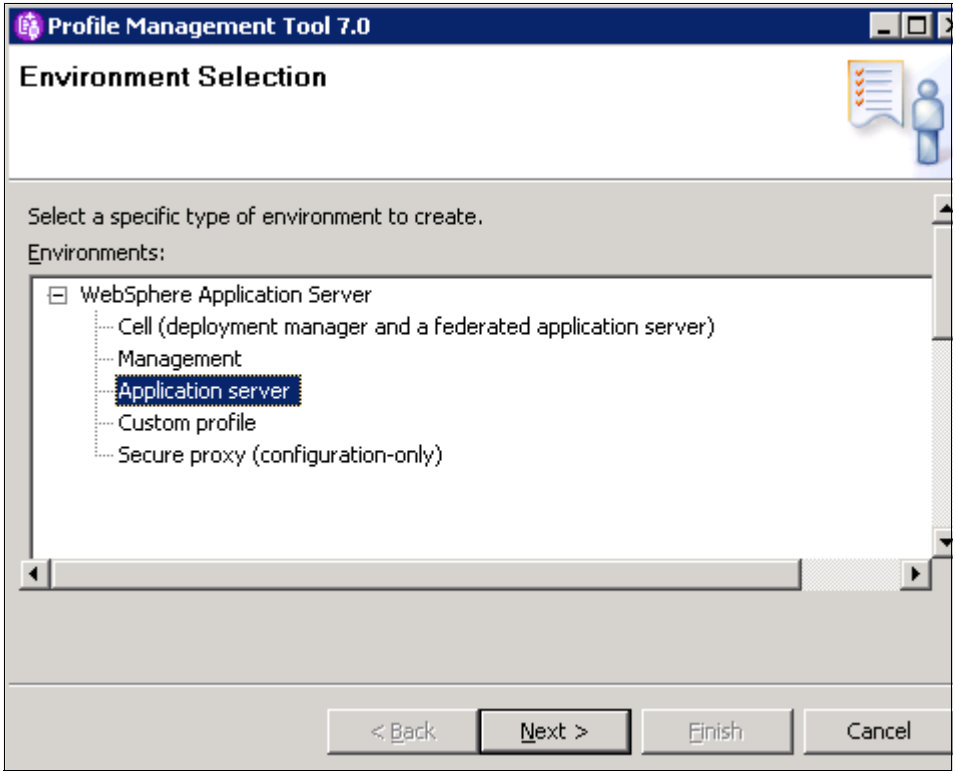

Figure 5 Pick Application server

The profile options are listed next. Note that the deployment manager profile is under the Management option, along with the new profile types for flexible management (administrative agent and job manager):

- Cell (deployment and a federated application server)
- Management:
  - Administrative agent ***(New in V7)***
  - Deployment manager
  - Job manager ***(New in V7)***
- Application server
- Custom profile
- Secure proxy (configuration-only) ***(New in V7)***

Profile creation options

While creating profiles, you are presented with a choice (Figure 6) of following the “Typical” path, where a set of default values for most settings will be used, or an “Advanced” path, which lets you specify values for each option.

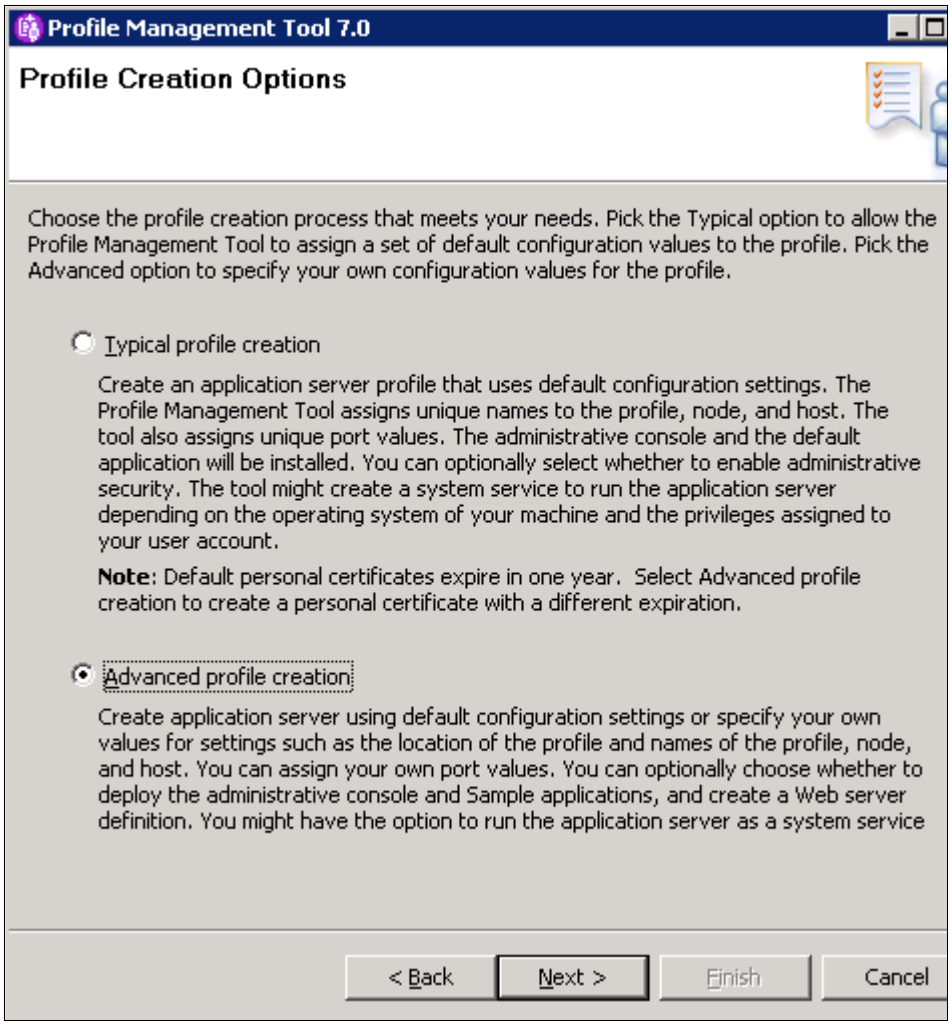

Figure 6 Profile creation path (typical as opposed to advanced option)

The Advanced path is preferred, because it gives you additional control over names and settings. An overview of the Advanced profile options is shown in Table 1.

Table 1 Options available in the typical versus advanced path

Option	Application Server	Deployment manager	Administra-tive Agent	Job manager	Custom	Cell
Deploy Administrative Console	Yes	Yes	Yes	Yes	No	Yes
Default and Sample Applications	Yes	No	No	No	No	Yes
Profile Name and Location	Yes	Yes	Yes	Yes	Yes	Yes
Node and Host Names	Yes	Yes	Yes	Yes	Yes	Yes
Administrative Security	Yes	Yes	Yes	Yes	Yes (Federation)	Yes
Certificates (part 1 and 2)	Yes	Yes	Yes	Yes	Yes	Yes
Port Assignment	Yes	Yes	Yes	Yes	Yes	Yes (Part 1 and part 2, one for dmgr and the other for App Server)
Windows Services (Windows only)	Yes	Yes	Yes	Yes	Yes	Yes
Web Server definition (Parts 1 and 2)	Yes	No	No	No	No	Yes
Summary	Yes	Yes	Yes	Yes	Yes	Yes

Profile name and location (and default profiles)

The wizard asks for a profile name and where you want the profile configuration files stored.

Directory location

By default, profiles are stored in *install_root*/profiles/*profile_name*. The logs for the process defined by the profile will reside within this directory structure; however, you can easily change this if space is a concern.

Default profile

The first profile that you create on a machine is the default profile. The default profile is the default target for commands that are issued from the bin directory in the product installation root when the -profileName argument is not used.

You can make another profile the default profile when you create that profile by checking **Make this profile** the default on the Profile name and location panel of the Advanced profile creation path. You can also make another profile the default profile using the **manageprofiles** command after you create the profile.

Profile name

The profile name must be unique within the installation and must follow an appropriate naming convention so you can easily identify it by the name it is given. The guidelines are as follows:

- Double-byte characters are supported.
- The profile name can be any unique name with the following restrictions.
- Do not use any of the following characters when naming your profile:
  - Spaces
  - Special characters that are not supported within the name of a directory on your operating system, such as asterisk (*), ampersand (&), or question mark (?)
  - Slashes (/) or (\)

Administrative security

When you create a profile for a process with the administrative functions (basically everything but a custom profile), you have the opportunity to enable administrative security. If you enable security during profile creation, you are asked for a user ID and password that will be added to a file-based user registry with the Administrator role.

We recommend that you enable administrative security. The file-based repository created during profile creation can be federated with other repositories later to provide a robust user registry for both administrative and application security.

Note: If you are going to create a job manager and register a deployment manager, keep in mind that you cannot register a deployment manager that has security enabled to a job manager that does not. So, you need to plan for administrative security across the WebSphere environment.

You can find more information about administrative security in Chapter 5, *Administration consoles and commands*.

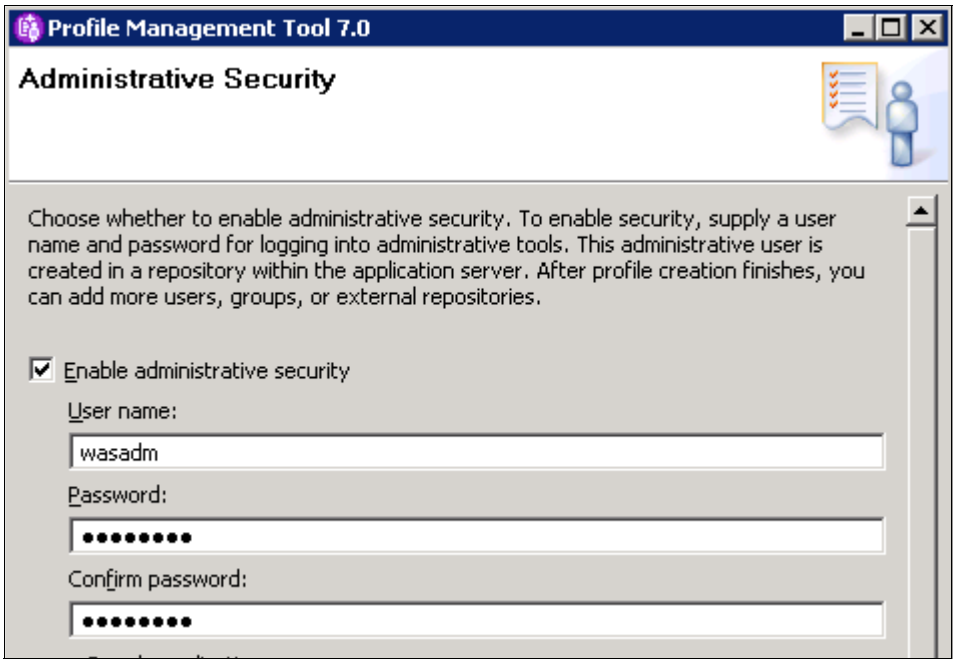

Figure 7 Enable administrative security

Certificates

Each profile contains a unique chained certificate signed by a unique long-lived root certificate that is created when the profile was created. When a profile is federated to a deployment manager, the signer for the root signing certificate is added to the common truststore for the cell, establishing trust for all certificates signed by that root certificate.

For a full description of the certificates and the keystore password, see:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.base.doc/info/aes/ae/csec_7ssldefault_chainedcert_config.html

Two panels are used during profile creation to manage the import or creation of these certificates.

The first panel (Figure 8) allows you to create the certificates or import existing certificates.

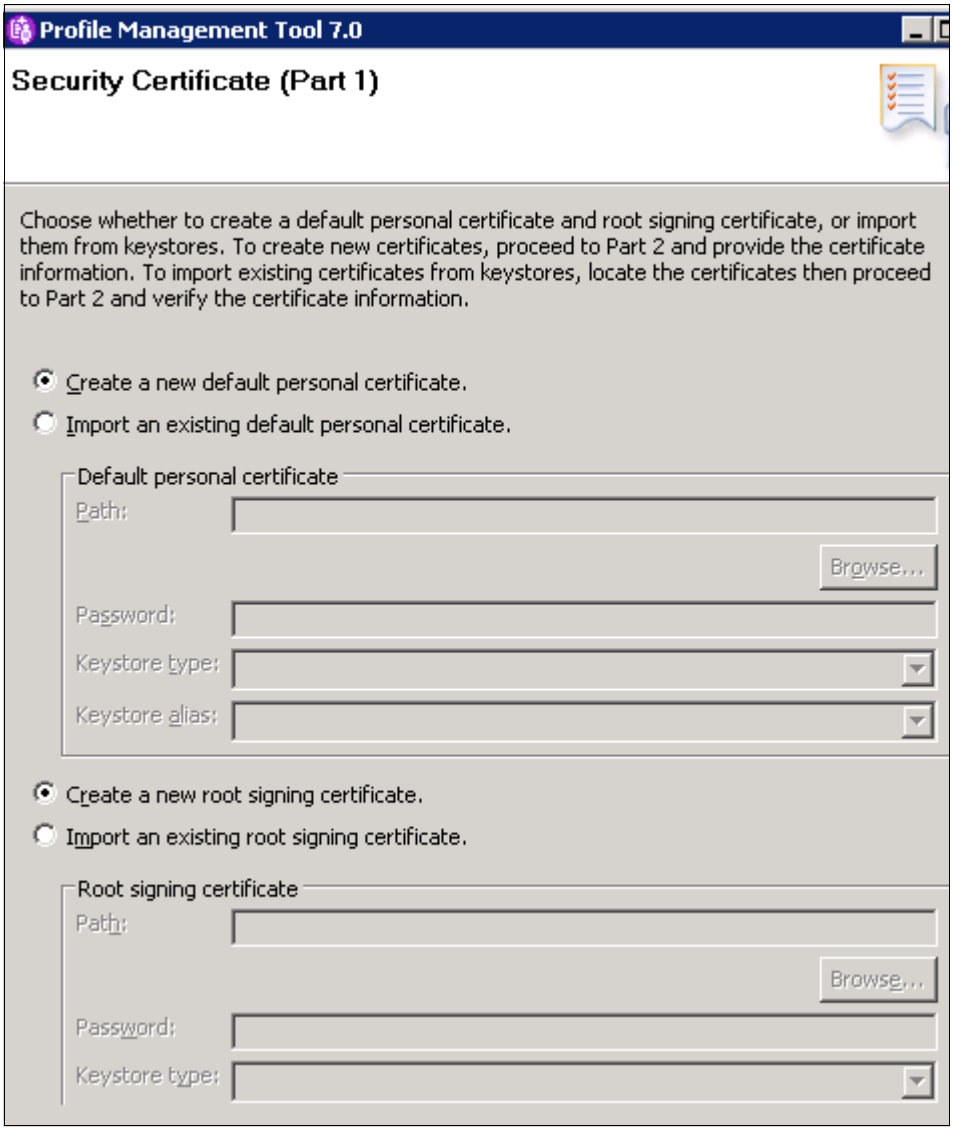

Figure 8 Create certificates or import existing personal or root certificates

The second panel (Figure 9) is used to modify the certificate information to create new certificates during profile creation. Review the expiration period and provide a new password for the default keystore. The default password is WebAS.

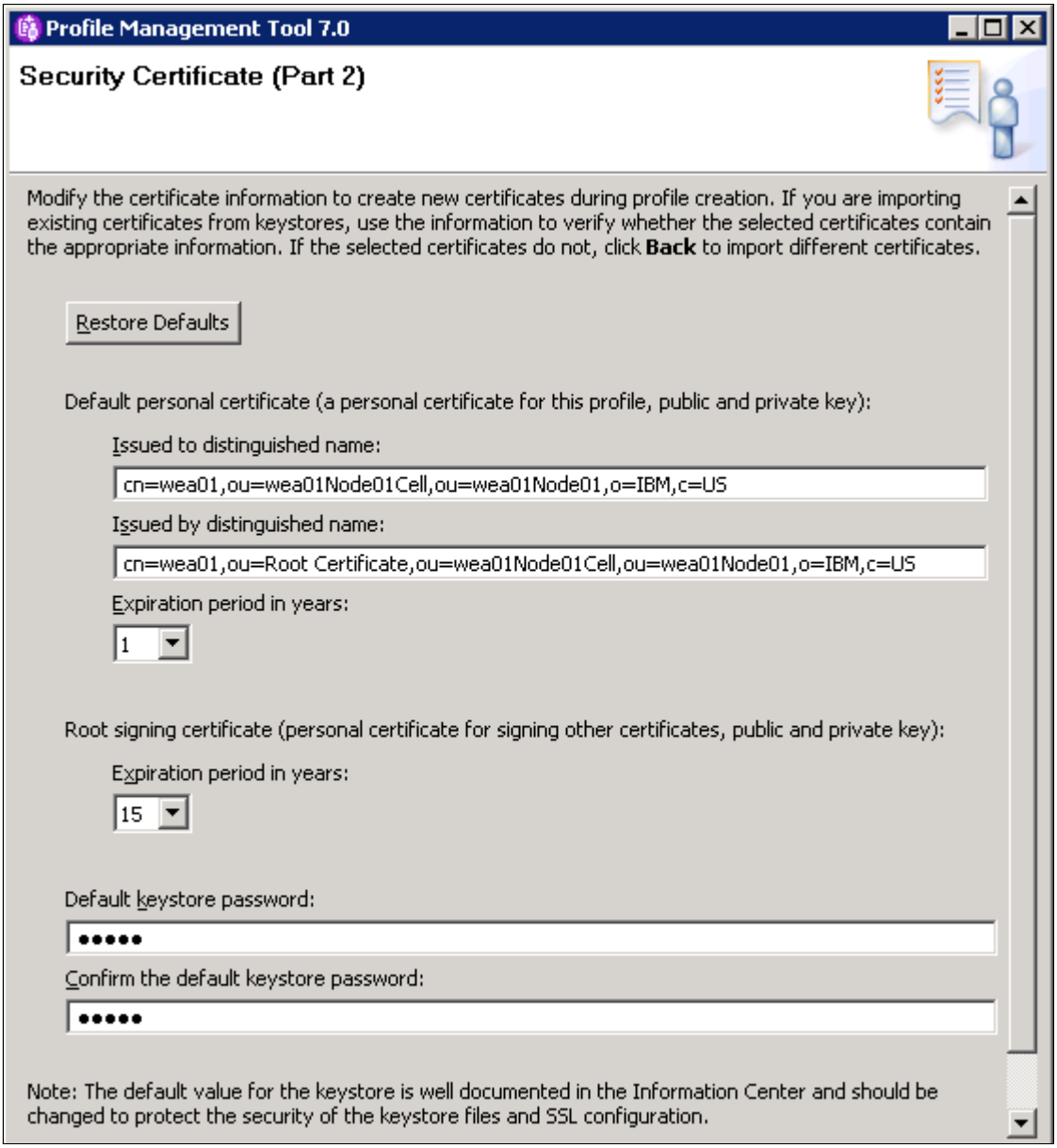

Figure 9 Modify certificate information at profile creation time

Port assignments

Every process uses a set of ports at runtime. These ports must be unique to a system. For the default port assignment for the distributed platform, see:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.migration.nd.doc/info/ae/ae/rmig_portnumber.html

The PMT wizard assigns unique port numbers to each profile if multiple profiles are installed in the same system. Careful planning is needed so that there are no port conflicts with other software installed on the same systems.

When you take the Advanced path through the profile wizard, you have three options:

- Use the default set of port numbers.
- Use the recommended set of port numbers. These have been selected as unique to the WebSphere installation.
- Customize the port numbers.

Run as a Windows service

When you create a profile on a Windows system, you have the option of running the application server as a Windows service. This provides you a simple way of automatically starting the server process when the system starts.

If you want to run the process as a Windows service, check the box and enter the values for the logon and startup type. Note that the window lists the user rights that the user ID you select needs to have. If the user ID does not have these rights, the wizard automatically adds them.

When you take the Typical path through the profile creation wizard, the default is to define the process as a Windows service (Figure 10 on page 18).

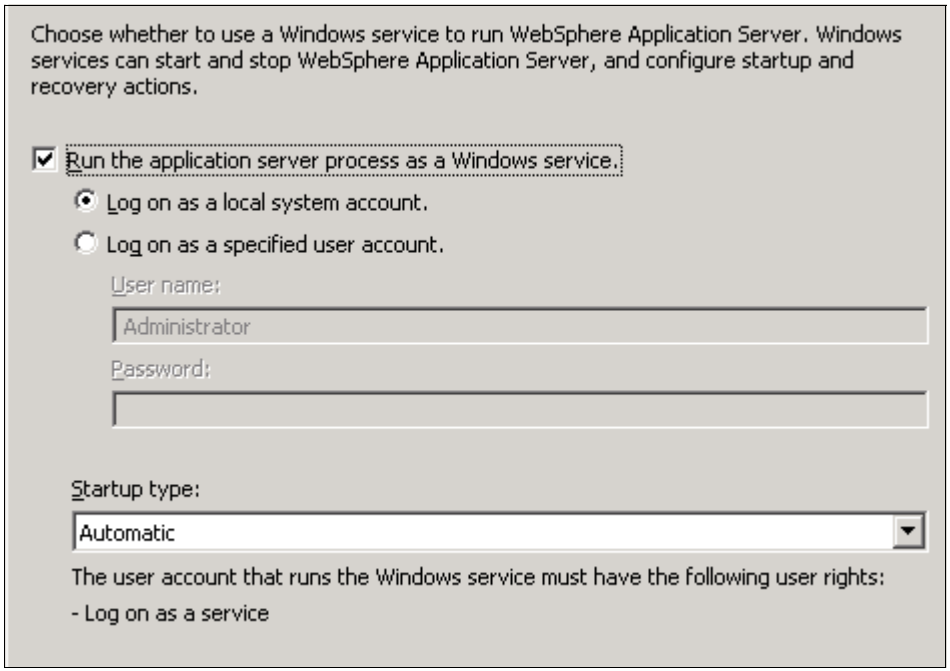

Figure 10 Run as a service

If you do not register the process as a Windows service during profile creation, you can do that later using the **WASService** command. For more information about the **WASService** command, see:

- **WASService** command

  http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/rins_wasservice.html

Verification steps

The profile will be stored in the directory structure you selected. In this IBM Redbooks publication, we refer to this directory as *profile_root*. This is where you can find, among other things, the `config` directory containing the configuration files, the `bin` directory for entering commands, and the `logs` directory where information is recorded.

After you create a new profile, you can take the following steps to verify that the profile is working correctly:

- View the messages produced by the profile creation.

  First, note the messages that result from the profile creation (Figure 11).

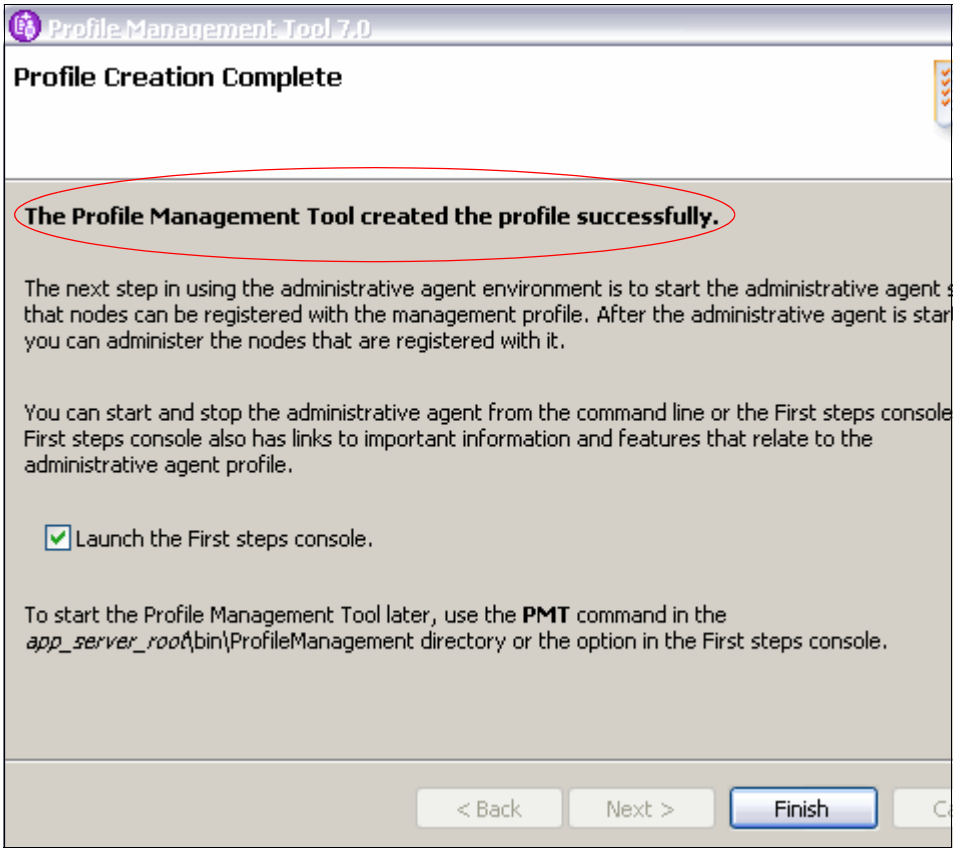

Figure 11 Profile creation complete - messages

If the messages indicate that the profile was not created successfully, look in the *install_root*/logs/manageprofiles/*profile_name*_create.log file to determine what went wrong.

Troubleshooting information can be found at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.installation.base.doc/info/aes/ae/tins_trouble.html

- Run the installation verification test:

  Each profile has its own IVT program that starts the process defined by the profile and runs a series of verification tests. The IVT program scans the `SystemOut.log` file for errors and verifies core functionality of the profile.

  Use the First Steps console to run the installation verification tests (IVT). The First Steps console starts by default when you click **Finish** at end of the profile creation. You can start the First Steps console any time by using the **`firststeps`** command located in the *`profile_root`*`/firststeps` directory. The options on this console vary depending on the profile type.

  Alternatively, the **`ivt`** command can be executed from the *`profile_root`*`/bin`. The IVT program verifies that the installation of the application server or deployment manager profile was successful.

  Messages from the IVT are displayed on the First Steps window and logged in the following places:

  - *`profile_root`*`/logs/`*`server_name`*`/startServer.log`
  - *`profile_root`*`/logs/`*`server_name`*`/SystemOut.log`

- If applicable, log in to the administrative console hosted by the process. You can access the console from the First Steps menu or by accessing its URL from a Web browser:

  `http://`*`server_host`*`:<`*`admin_console_port`*`>/ibm/console`

  Here is a sample URL:

  `http://localhost:9060/ibm/console/`

  The administrative console port is selected during profile creation (see Figure 16 on page 25).

  Click the **Log in** button. If you did not enable security, you do not have to enter a user name. If you choose to enter a name, it can be any name. It is used to track changes you make from the console. If you enabled administrative security, enter the user ID and password you specified.

Figure 12 shows the First steps console for a standalone application server.

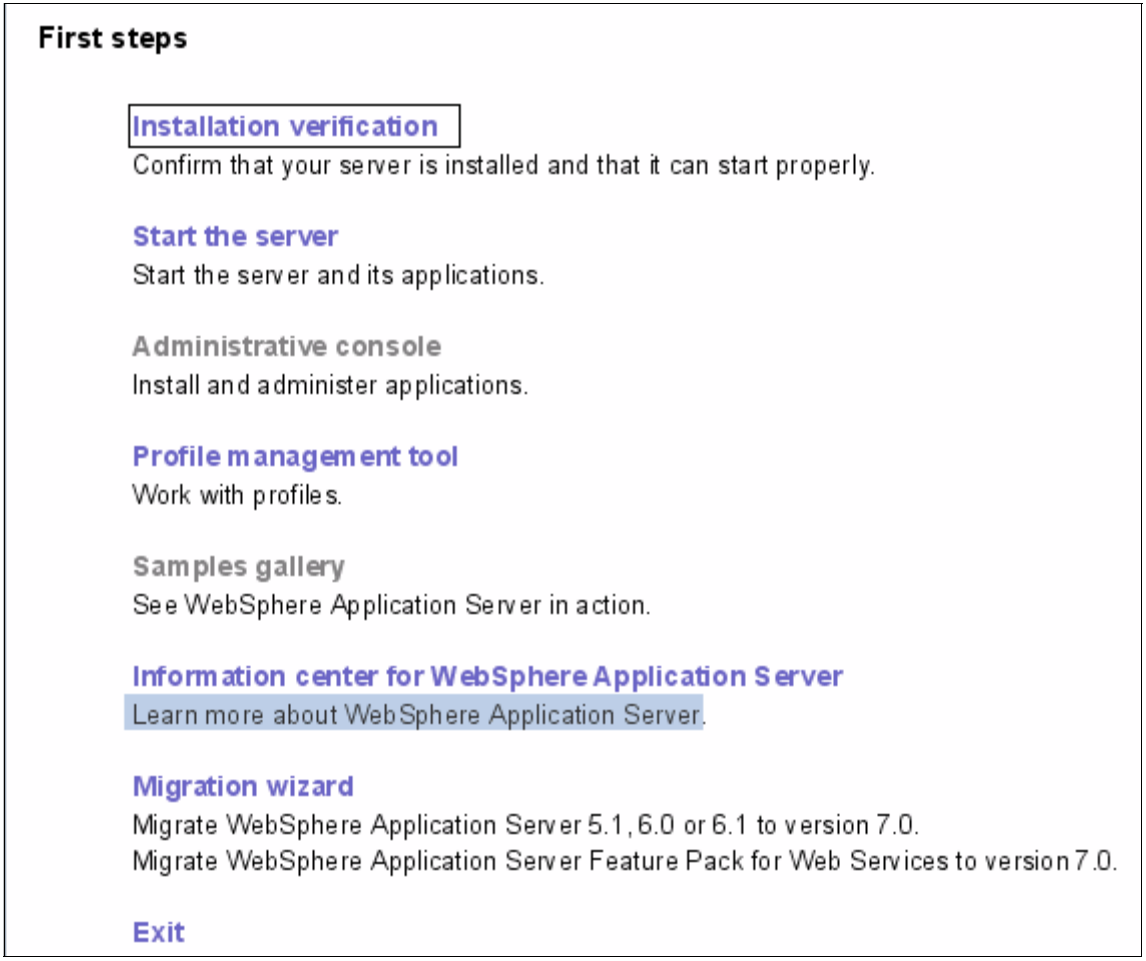

Figure 12 First Steps

Creating an application server profile

An application server profile defines a new standalone application server. This server can be run standalone or can be later federated to a deployment manager cell for central management.

This section takes you through the steps of creating the application server profile: It shows the steps in the Advanced path through the profile creation:

1. Start the Profile Management Tool and click **Launch Profile Management Tool** on the Welcome page.

2. Click the **Create** button.
3. Select **Application server** as the profile type and click **Next.**
4. Select **Advanced**. Click **Next**.
5. Select the applications you want to deploy (Figure 13).

   Installing the administrative console is recommended. However, there might be some circumstances when you would not want to install an administrative console, such as, if you plan to control all administrative tasks via scripting.

   WebSphere Application Server provides sample applications that you can use to familiarize yourself with WebSphere applications. If you have installed the sample applications (optional during WebSphere Application Server installation), you can opt to deploy these to the server during profile creation. For information about the samples available and how to install them, see the topic, *Accessing the Samples*, under *Learn about WebSphere Applications*, in the Information Center:

   `http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/welc6tech.html`

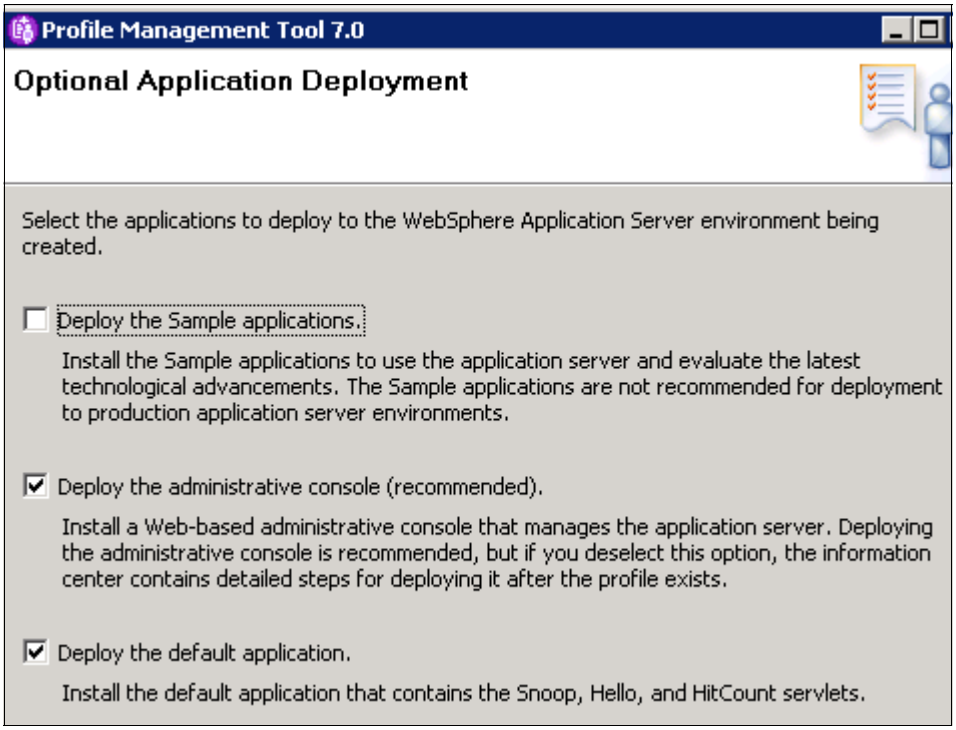

Figure 13 Select applications required

Click **Next**.

6. Enter a unique name for the profile or accept the default. If the application server will be used primarily for development purposes, check the option to create it from the development template. The development template reduces startup time and allows the server to run on less powerful hardware. Do not use this for production servers (Figure 14).

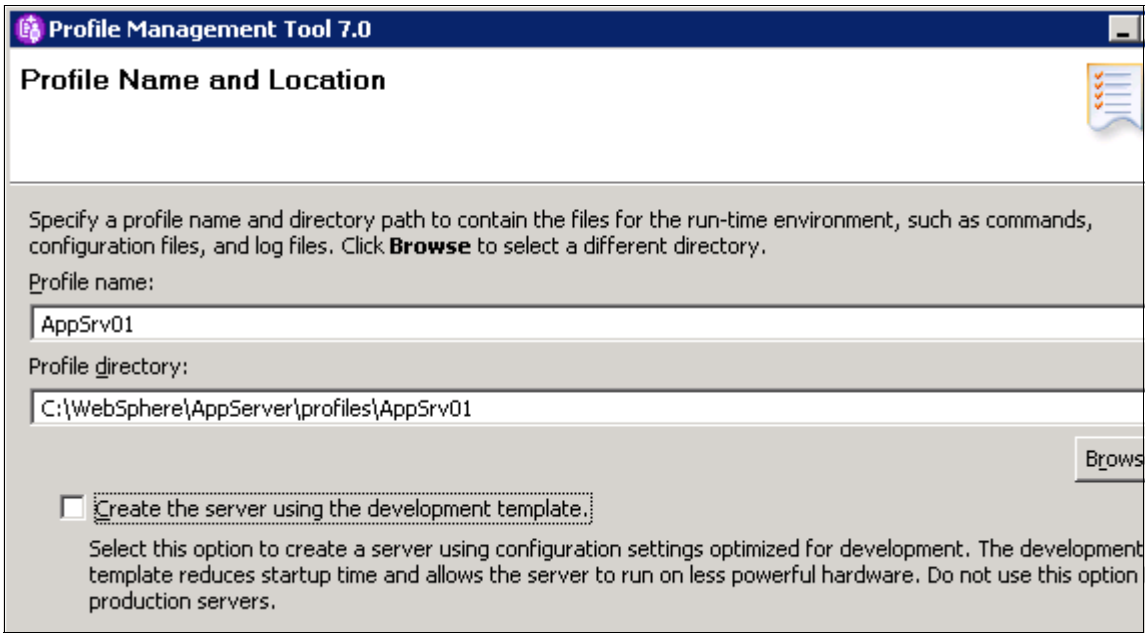

Figure 14 Enter name and location

Click **Next.**

7. Enter the new node name and the system host name. The node name will default based on the host name of your system. The wizard recognizes if there are existing nodes in the installation and takes this into account when creating the default node name (Figure 15 on page 24).

Note: If you are planning to create multiple standalone application servers for federation later to the same cell, make sure that you select a unique node name for each application server.

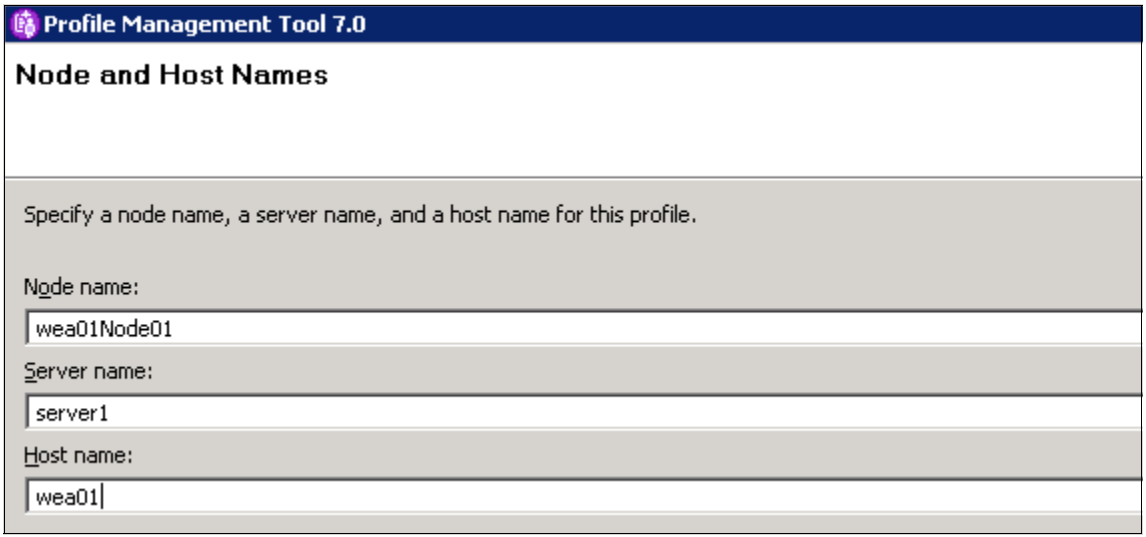

Figure 15 Enter host and node names

Click **Next**.

8. Choose whether to enable administrative security. If you enable security, you are asked for a user ID and password that will be added to a file-based user registry with the Administrator role.

   You are asked for a password for the samples if you checked the earlier option to include the samples in this application server.

   Important: It might seem obvious, but do make a note of the user ID and passwords you enter here. Without the administrator ID, you will not be able to manage the application server.

   Click **Next**.

9. Elect to either create new default personal and root signing certificates or to import them.

   Click **Next**.

10. Review and modify the certificate information as needed.

    Click **Next**.

11. The wizard presents a list of TCP/IP ports for use by the application server. If you already have existing profiles on the system (within this installation), this is taken into account when the wizard selects the port assignments, but you should verify that these ports will be unique on the system. You can select a different port by using the up and down arrows next to the port number.

Figure 16 shows some typical port assignments.

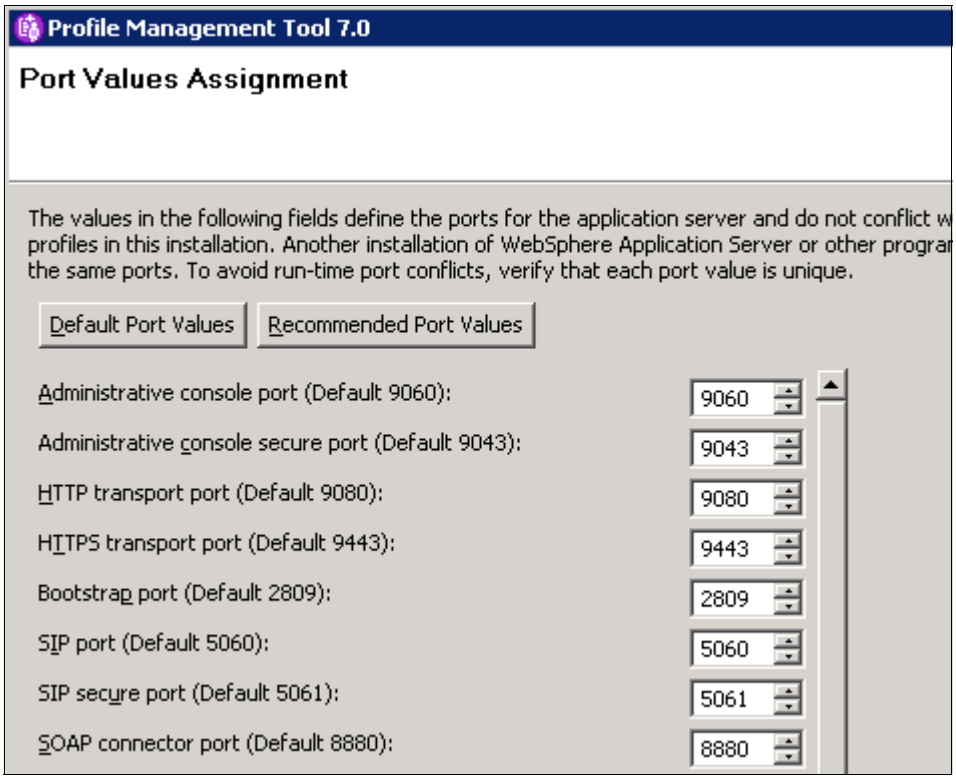

Figure 16 Select ports

Important: Make a note of the following port numbers for later use:

- *SOAP connector port:* If you plan to federate this node to a deployment manager later using the deployment manager administrator console, you need to know this port number. This is also the port that you connect to when using the **`wsadmin`** administration scripting interface.
- *Administrative console port:* You need to know this port in order to access the administrative console. When you turn on security, you need to know the *Administrative console secure port.*
- *HTTP transport port:* This port is used to access applications running on the server directly as opposed to going through a Web server. This is useful in test environments.

Click **Next.**

12. If the profile is being created on a Windows system, select whether you want the server to run as a Windows service.

    Click **Next**.

13. The wizard allows you to create an optional Web server definition (Figure 17). Web server definitions define an external Web server to WebSphere Application Server. This allows you to manage Web server plug-in configuration files for the Web server and in some cases to manage the Web server. If you have not installed a Web server or want to do this later, you can easily do this from the administrative console.

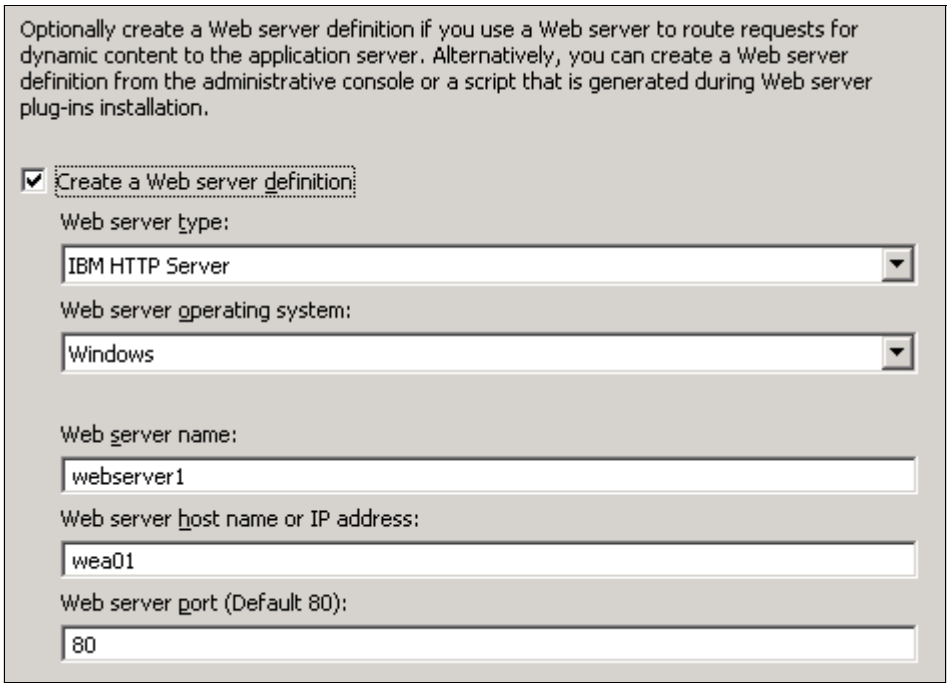

Figure 17 Creating a Web Server definition

Click **Next.**

14. If you elect to create a Web server definition, the next panel shows the default locations of the Web server installation and Web server plug-in path. Change this to match your installation (Figure 18).

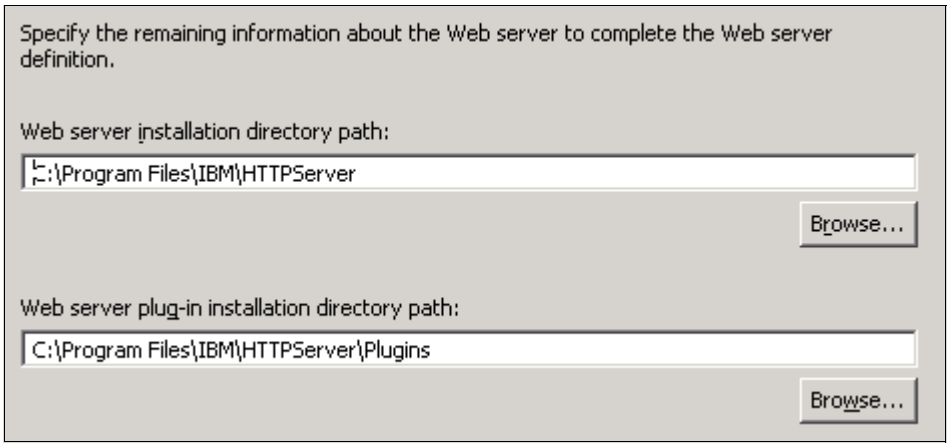

Figure 18 Location of Web server definition

Click **Next**.

15. Review the options you have chosen and click **Next** to create the profile.
16. The final window indicates the success or failure of the profile creation. If you have errors, check the log at:

    install_root/logs/manageprofiles/*profile_name*_create.log

    You can also find logs for individual actions stored in:

    profile_root/logs
17. Click **Finish** to close the wizard and start the First Steps application.
18. Use the First Steps console to verify the installation, start the server, and log in to the administrative console.

19. Display the configuration from the console. You should be able to see the following items from the administrative console:

    a. Application servers:

       Select **Servers** → **Server Types** → **WebSphere Application servers**. You should see the application server in the list (Figure 19).

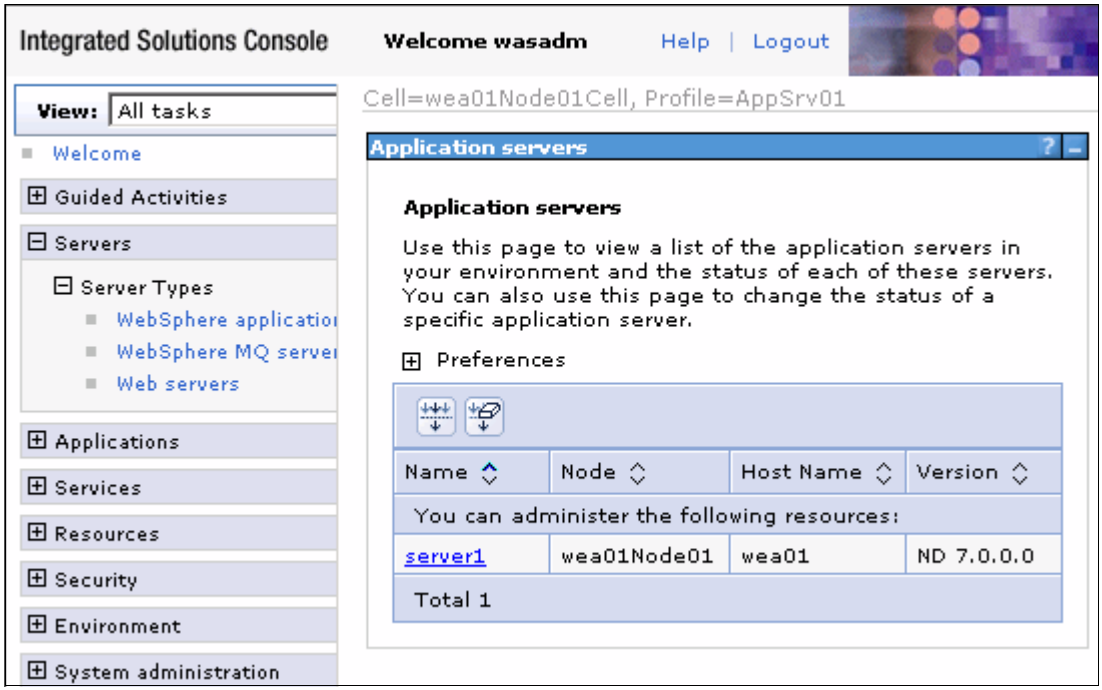

Figure 19 Application server defined by the application server profile

To see the configuration of this server, click the name in the list.

b. Enterprise applications:

Select **Applications** → **Application Types** → **WebSphere enterprise applications**. You should see a list of applications. Figure 20 shows the WebSphere sample applications.

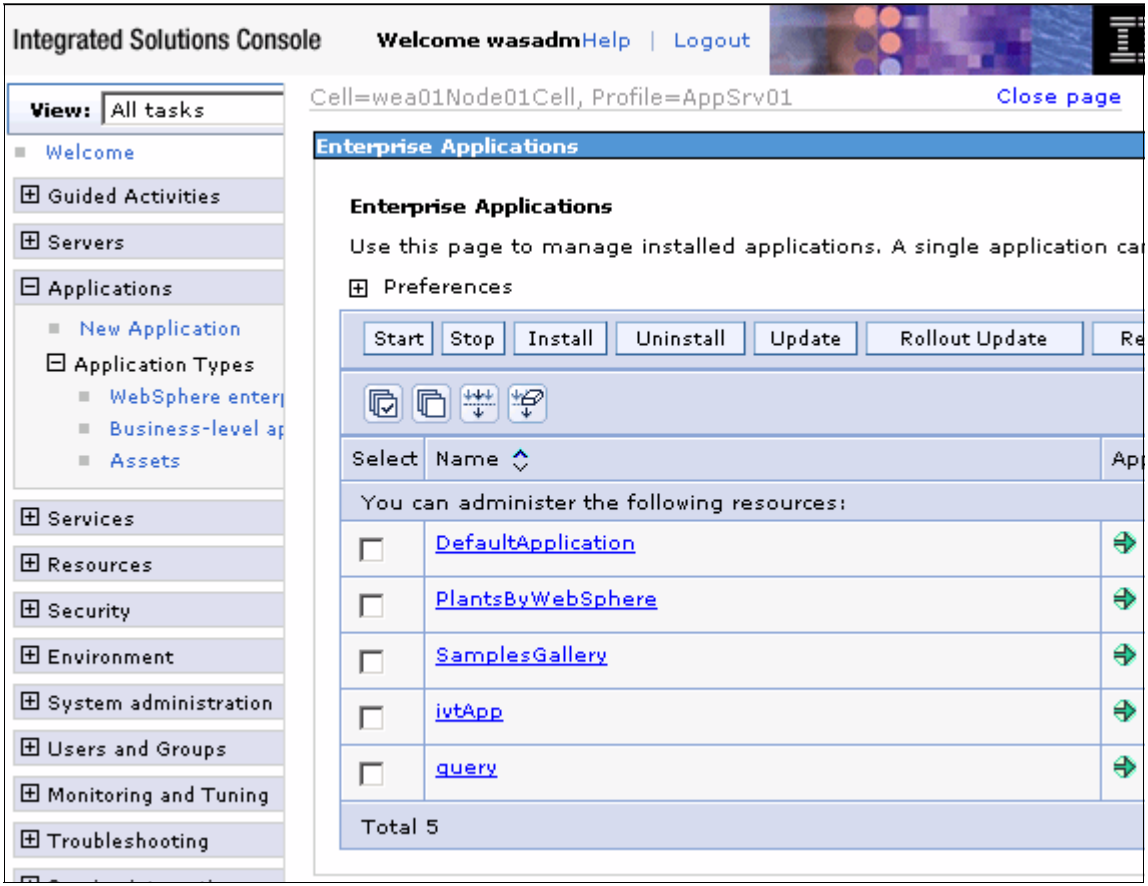

Figure 20 Applications installed on server1

Working with application servers: For information about starting, stopping, and viewing application servers, see Chapter 6, *Administration of WebSphere processes*.

Creating a deployment manager profile

The following steps outline the process of creating a deployment manager profile (Figure 21):

1. Start the PMT and click the **Launch Profile Management Tool** button on the Welcome page.
2. Click **Create**.
3. Select **Management**. Click **Next**.
4. Select **Deployment manager**. Click **Next**.
5. Select whether to take the typical settings or to go through the advanced windows. The options that you see next depend on the path you take.

   If **Typical** is selected, you only see one more option (to enable security).

   If **Advanced** is selected, you continue with the following steps.
6. Select the option to deploy the administrative console (the default) and click **Next**.
7. Enter a unique name for the profile or accept the default. The profile name becomes the directory name for the profile files. Click the box if you want this to be the default profile for receiving commands. Select the location for the profile and click **Next**.

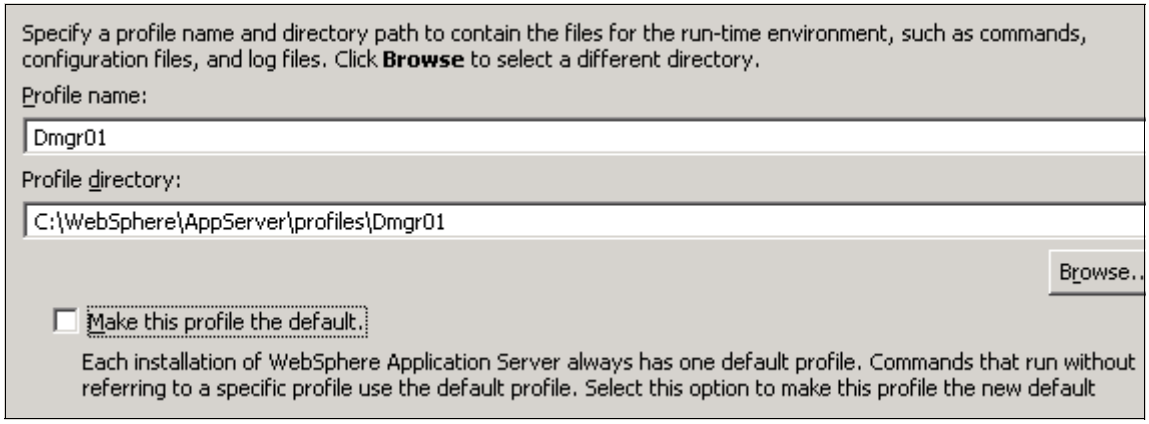

Figure 21 Creating a deployment manager profile: Enter name and location

8. Enter the node, host, and cell names. These default, based on the host name of your system. The wizard recognizes if there are existing cells and nodes in the installation and takes this into account when creating the default names. Click **Next** (Figure 22).

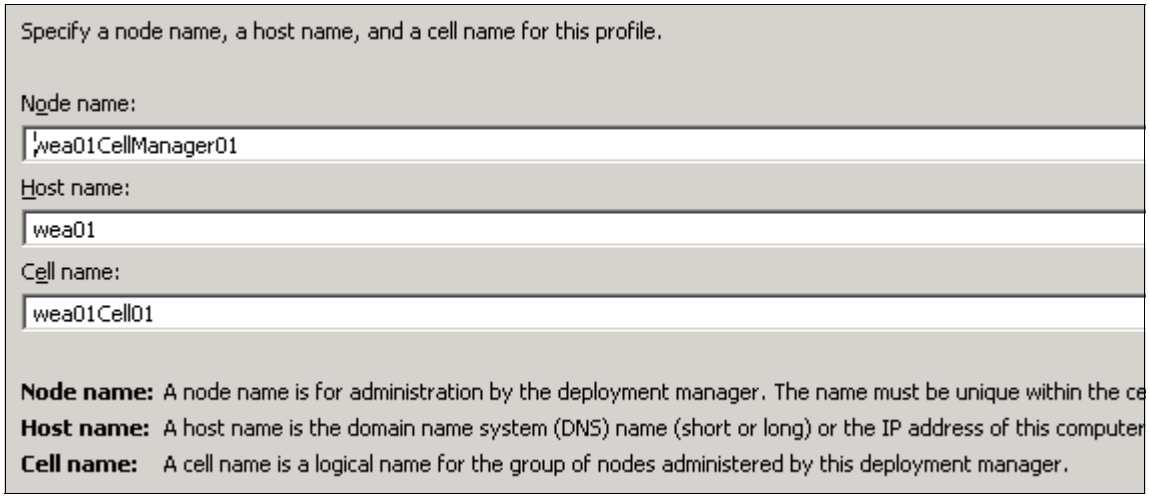

Figure 22 Creating a deployment manager profile: Enter cell, host, and node names

9. Choose whether to enable administrative security. If you enable security here, you are asked for a user ID and password that will be added to a file-based user registry with the Administrator role. Click **Next**.
10. Elect to either create new default personal and root signing certificates or to import them.

    Click **Next**.
11. Review and modify the certificate information as needed.

    Click **Next**.
12. The wizard presents a list of TCP/IP ports for use by the deployment manager. If you already have existing profiles on the system, this is taken into account when the wizard selects the port assignments. However, you should verify that these ports will be unique on the system (Figure 23).

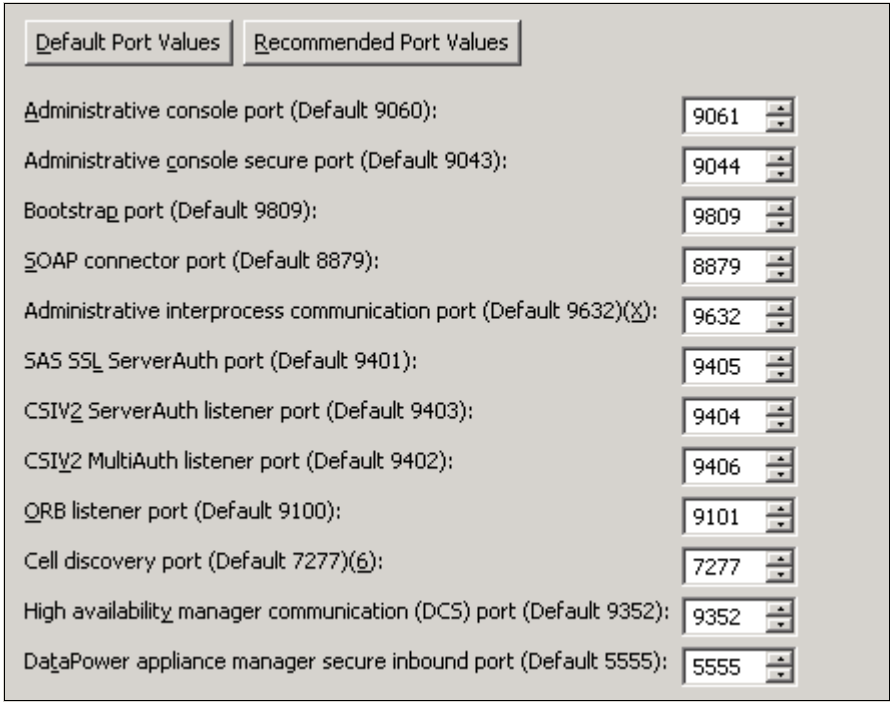

Figure 23 Creating a deployment manager profile: Select ports

Note two ports: You might want to note the following ports for later use:

- *SOAP connector port*: If you use the **addNode** command to federate a node to this deployment manager, you need to know this port number. This is also the port you connect to when using the **wsadmin** administration scripting interface.
- *Administrative console port:* You need to know this port in order to access the administrative console. When you turn on security, you need to know the *Administrative console secure port*.

13. If you would like to run the process as a Windows service, leave the box checked and enter the values for the logon and startup type.

    Click **Next**.

14. Review the options that you have chosen (Figure 24). If you took the Typical path through the wizard, make sure that the default selections suit your needs. Click **Create** to create the profile.

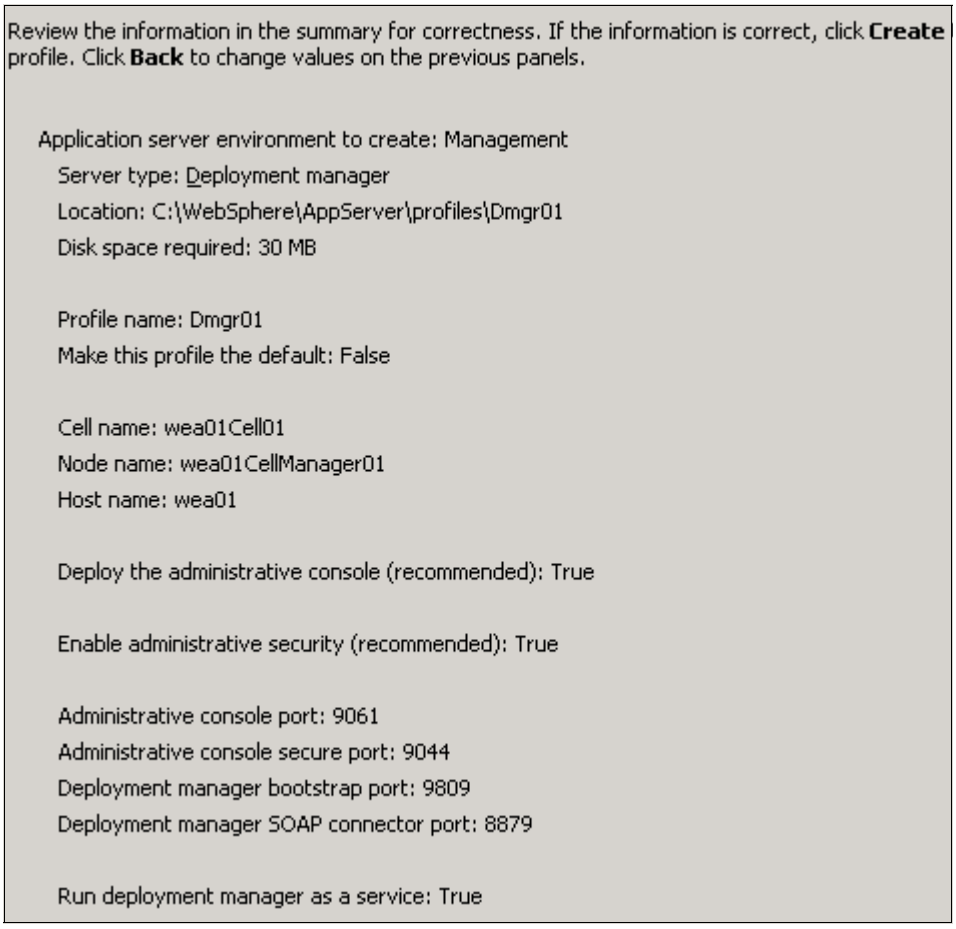

Figure 24 Creating a deployment manager profile: Finish

15. The final window indicates the success or failure of the profile creation. If you have errors, check the log at:

    install_root/logs/manageprofiles/*profile_name*_create.log

    You can also find logs for individual actions stored in:

    profile_root/logs

16. Click **Finish** to close the wizard and start the First Steps application.

17. Verify the installation. You can do this directly from the First Steps menu. The IVT process starts the deployment manager and checks the log file for warnings or errors on start.

18. Open the administrative console by selecting the option in the First Steps window, or by accessing its URL from a Web browser:

    `http://<dmgr_host>:<admin_console_port>/ibm/console`

    Here is a sample URL in the address bar:

    `http://localhost:9060/ibm/console/`

19. Log in and display the configuration from the console. You should be able to see the following items from the administrative console:

    a. Cell information: Select **System administration** → **Cell**.

    b. Deployment manager: Select **System administration** → **Deployment manager**.

    c. Deployment manager node: Select **System administration** → **Nodes**.

    d. The default node group: Select **System administration** → **Node groups**.

    Note that at the completion of this process you do not have:

    a. A node agent:

       Node agents reside on nodes with managed application servers. You do not see node agents appear until you federate a node to the cell.

    b. Application servers

Working with deployment managers: For information about starting, stopping, and viewing deployment managers, see Chapter 6, *Administration of WebSphere processes*.

Creating a cell profile

Table 2 shows a summary of the options you have during a cell profile creation. Using this option actually creates two distinct profiles: a deployment manager profile and an application server profile. The application server profile is federated to the cell. The options you see are a reflection of the options you would see if you were creating the individual profiles versus a cell. The PMT panels give you basically the same options that you would see if you created a deployment manager, then an application server.

Table 2 Cell profile options

Typical	Advanced
The administrative console and default application are deployed by default. The sample applications are not deployed.	You have the option to deploy the administrative console (recommended), the default application, and the sample applications (if installed).
The profile name for the deployment manager is Dmgr*xx* by default, where *xx* is 01 for the first deployment manager profile and increments for each one created. The profile is stored in *install_root*/profiles/Dmgr*xx*.	You can specify the profile name and its location.
The profile name for the federated application server and node is AppSrv*xx* by default, where *xx* is 01 for the first application server profile and increments for each one created. The profile is stored in *install_root*/profiles/AppSrv*xx*.	You can specify the profile name and its location.
Neither profile is made the default profile.	You can choose to make the deployment manager profile the default profile.
The cell name is <*host*>Cell*xx*. The node name for the deployment manager is <*host*>CellManager*xx.* The node name for the application server is <*host*>Node*xx*. The host name is prefilled in with your system's DNS host name.	You can specify the cell name, the host name, and the profile names for both profiles.
You can enable administrative security (yes or no). If you select yes, you are asked to specify a user name and password that will be given administrative authority.	
TCP/IP ports default to a set of ports not used by any profiles in this WebSphere installation instance.	You can use the recommended ports for each profile (unique to the installation), use the basic defaults, or select port numbers manually.
(Windows) The deployment manager will be run as a service.	(Windows) You can choose whether the deployment manager will run as a service.
Does not create a Web server definition.	Allows you to define an external Web server to the configuration.

Creating a custom profile

A custom profile defines an empty node on a system. The purpose of this profile is to define a node on a system to be federated to a cell for management through a deployment manager.

As you create the profile, you have the option to federate the node to a cell during the wizard, or to simply create the profile for later federation. Before you can federate the custom profile to a cell, you need to have a running deployment manager.

Note: With other profiles, you have the option of registering the processes as Windows services. This does not appear as an option when you create a custom profile.

The following steps outline the process of creating a custom profile (Figure 25):

1. Start the Profile Management Tool and click the **Launch Profile Management Tool** button on the Welcome page.
2. Click **Create**.
3. Select **Custom profile**. Click **Next**.
4. Select whether to take the typical settings or to go through the advanced windows. The options you see next depend on the path you take.

   If **Typical** is selected, you only see one more option (to enable security).

   If **Advanced** is selected, you continue with the following steps.
5. Enter a unique name for the profile or accept the default. The profile name becomes the directory name for the profile files.

   Click the box if you want this directory to be the default profile for receiving commands. Click **Next**.

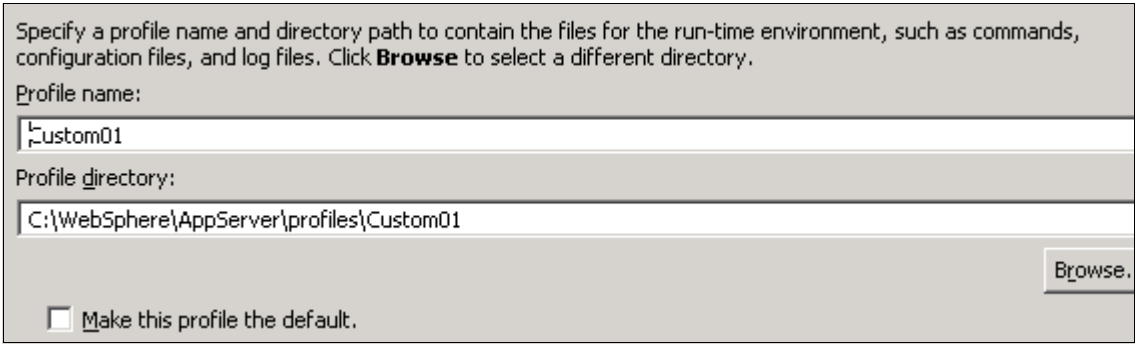

Figure 25 Creating a Custom profile: Enter name and location

6. Enter the new node name and the system host name. The node name defaults to the host name of your system. The wizard recognizes if there are existing nodes in the installation and takes this into account when creating the default node name. Click **Next** (Figure 26).

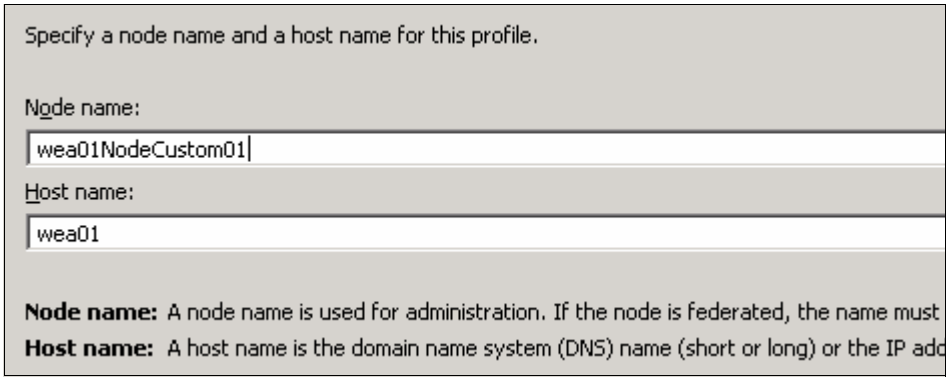

Figure 26 Creating a custom profile: Enter host and node names

7. If you would like to federate the new node defined by the profile to a cell as part of the wizard process, leave the “Federate this node later” box unchecked and enter the host name and SOAP connector port for the deployment manager. Enter the user ID and password of the administrator ID for the deployment manager.

   Click **Next**.

   When you click **Next**, a connection is attempted to the deployment manager. If you have entered any of these values incorrectly, you will be able to correct them (Figure 27).

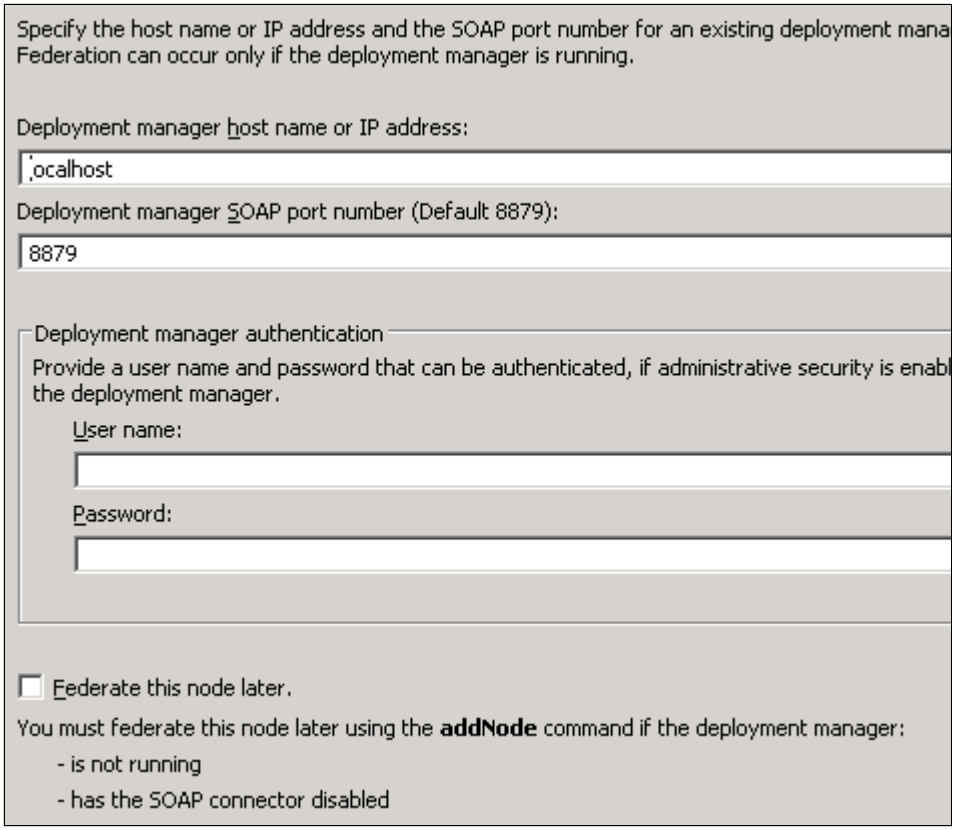

Figure 27 Creating a custom profile: Federate later

8. Review the options you have chosen. If you took the Typical path through the wizard, make sure that the default selections suit your needs (Figure 28).

Figure 28 Creating a custom profile: Summary

Click **Create** to create the profile.

9. The final window indicates the success or failure of the Custom profile creation.

   If you have errors, check the log at:

   install_root/logs/manageprofiles/*profile_name*_create.log

   Note that you will have to click **Finish** on the window to unlock the log.

   You can also find logs for individual actions stored in:

   profile_root/logs

Note: Custom profiles do not create a server process, so you cannot verify, stop, or start the profile. The only reason to launch the First Steps menu is if you want to link to the Information Center or launch the migration wizard.

10. The federation process creates a node agent for the new node, federates it to the cell, and starts the node agent. If you federated the custom profile, open the deployment manager administrative console and view the node and node agent:
    - Select **System Administration** → **Nodes**. You should see the new node.
    - Select **System Administration** → **Node agents**. You should see the new node agent.

– Select **System Administration** → **Cells.** Click the **Local Topology** tab and expand the view. From here, you can see a tree diagram of the cell (Figure 29).

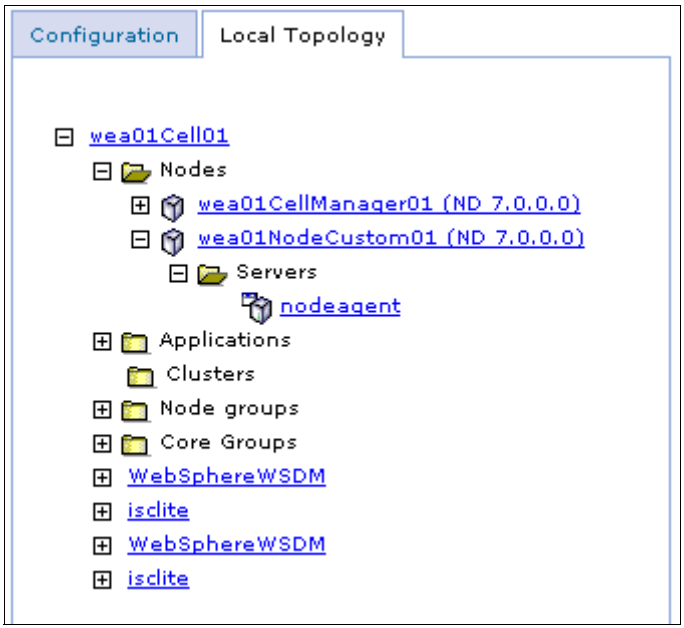

Figure 29 Topology view of a cell

If you have not federated the node, proceed to “Federating nodes to a cell” on page 40. Otherwise, you can continue by defining an application server on the new node (see Chapter 6, *Administration of WebSphere processes*).

Federating nodes to a cell

A custom profile defines a node that can be added to a cell. The **addNode** command is used to federate a node in a custom profile to a cell.

A standalone application server can also be federated to a cell with the **addNode** command, or from the deployment manager administrative console. The administrative console invokes the **addNode** command on the target system.

When you federate a node, the node name from the federated node is used as the new node name and must be unique in the cell. If the name of the node that you are federating already exists, the **addNode** operation will fail.

The addnode command

The **addNode** command is run from the *install_root*/bin or *profile_root*/bin directory of the installation for the profile that will be federated (that is, from the custom profile or application server profile installation).

Addnode command syntax

The syntax of the **addNode** command is shown in Example 1.

Example 1 addNode syntax

```
Usage: addNode dmgr_host [dmgr_port] [-conntype <type>] [-includeapps]
[-includebuses] [-startingport <portnumber>]
[-portprops <qualified-filename>] [-nodeagentshortname <name>]
[-nodegroupname <name>] [-registerservice] [-serviceusername <name>]
[-servicepassword <password>] [-coregroupname <name>] [-noagent]
[-statusport <port>] [-quiet] [-nowait] [-logfile <filename>]
[-replacelog] [-trace] [-username <username>] [-password <pwd>]
[-localusername <localusername>] [-localpassword <localpassword>]
[-profileName <profile>] [-excludesecuritydomains] [-help]
```

- `dmgr_host, -username, -password`

  This command connects to the deployment manager, so you have to specify the deployment manager host name and a user ID/password with administrative privileges on the deployment manager.

- `dmgr_port, -conntype`

  The default is to connect to the deployment manager using SOAP and port 8879. If your deployment manager was defined with this port, you do not need to specify anything. If not, you can specify the correct port, or you can use RMI as the connection type.

  For SOAP connections, the port defined as the SOAP_CONNECTOR_PORT number on the deployment manager must be specified. If you choose to use an RMI connection instead, the ORB_LISTENER_ADDRESS port must be specified. You can see these in the port list of the deployment manager in the administrative console.

  Tip: Port numbers are stored in *profile_root*/properties/portdef.props also.

- `-startingport, -portprops <`*filename*`>`

  The new node agent is assigned a range of ports automatically. If you want to specify the ports for the node rather than taking the default, you can specify a

starting port using the -startingport parameter. The numbers are incremented from this number.

For example, if you specify 3333, the BOOTSTRAP_ADDRESS port will be 3333, the CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS will be 3334, and so on.

As an alternative, you can provide specific ports by supplying a file with the port properties.

- `-includeapps, -includebuses`

  If you are federating an application server, you can keep any applications that are deployed to the server and you can keep any service integration bus definitions that have been created. The default is that these are not included during federation and are lost.

For more information about the **addNode** syntax and options, see:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/rxml_addnode.html

The **addNode** command performs the following actions:

1. Connects to the deployment manager process. This is necessary for the file transfers performed to and from the deployment manager in order to add the node to the cell.
2. Attempts to stop all running application servers on the node.
3. Backs up the current standalone node configuration to the *profile_root*/config/backup/base/ directory.
4. Copies the standalone node configuration to a new cell structure that matches the deployment manager structure at the cell level.
5. Creates a new local config directory and definition (server.xml) for the node agent.
6. Creates entries (directories and files) in the master repository for the new node's managed servers, node agent, and application servers.
7. Uses the FileTransfer service to copy files from the new node to the master repository.
8. Uploads applications to the cell only if the -includeapps option is specified.
9. Performs the first file synchronization for the new node. This pulls everything down from the cell to the new node.
10. Fixes the node's **setupCmdLine** and **wsadmin** scripts to reflect the new cell environment settings.
11. Launches the node agent (unless -noagent is specified).

Federating a custom node to a cell

Note: You only have to do this if you created a custom profile and chose *not* to federate it at the time. This requires that you have a deployment manager profile and that the deployment manager is up and running.

To federate the node to the cell, do the following actions:

1. Start the deployment manager.
2. Open a command window on the system where you created the custom profile for the new node. Switch to the *profile_root*/bin directory or *install_root*/bin directory.
3. Run the **addNode** command.

   Example 2 shows an example of using the **addNode** command on a Windows system to add Node01 to the deployment manager using 8879 as the SOAP connector address.

Example 2 addNode command

```
C:\WebSphere\AppServer\profiles\Custom01\bin>
C:\WebSphere\AppServer\profiles\Custom01\bin>addNode localhost 8879
ADMU0116I: Tool information is being logged in file
           C:\WebSphere\AppServer\profiles\Custom01\logs\addNode.log
ADMU0128I: Starting tool with the Custom01 profile
CWPKI0308I: Adding signer alias "CN=wea01, OU=Root Certificate, " to local
           keystore "ClientDefaultTrustStore" with the following SHA digest:
           AF:60:11:60:15:5B:B3:54:0C:46:84:1A:B5:DC:C6:A9:B6:DC:0F:0E
CWPKI0308I: Adding signer alias "datapower" to local keystore
           "ClientDefaultTrustStore" with the following SHA digest:
           A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17
ADMU0001I: Begin federation of node wea01NodeCustom01 with Deployment Manager
           at localhost:8879.
ADMU0009I: Successfully connected to Deployment Manager Server: localhost:8879
ADMU0507I: No servers found in configuration under:
           C:\WebSphere\AppServer\profiles\Custom01\config/cells/wea01Node02Cell
/nodes/wea01NodeCustom01/servers
ADMU2010I: Stopping all server processes for node wea01NodeCustom01
ADMU0024I: Deleting the old backup directory.
ADMU0015I: Backing up the original cell repository.
ADMU0012I: Creating Node Agent configuration for node: wea01NodeCustom01
ADMU0014I: Adding node wea01NodeCustom01 configuration to cell: wea01Cell01
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: wea01NodeCustom01
ADMU0020I: Reading configuration for Node Agent process: nodeagent
```

```
ADMU0022I: Node Agent launched. Waiting for initialization status.
ADMU0030I: Node Agent initialization completed successfully. Process id is:
           5368
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: nodeagent
ADMU0300I: The node wea01NodeCustom01 was successfully added to the wea01Cell01
           cell.
ADMU0306I: Note:
ADMU0302I: Any cell-level documents from the standalone wea01Cell01
           configuration have not been migrated to the new cell.
ADMU0307I: You might want to:
ADMU0303I: Update the configuration on the wea01Cell01 Deployment Manager with
           values from the old cell-level documents.
ADMU0306I: Note:
ADMU0304I: Because -includeapps was not specified, applications installed on
           the standalone node were not installed on the new cell.
ADMU0307I: You might want to:
ADMU0305I: Install applications onto the wea01Cell01 cell using wsadmin
           $AdminApp or the Administrative Console.
ADMU0003I: Node wea01NodeCustom01 has been successfully federated.
C:\WebSphere\AppServer\profiles\Custom01\bin>
```

4. Open the deployment manager administrative console and view the node and node agent:
   - Select **System Administration** → **Nodes**. You should see the new node.
   - Select **System Administration** → **Node agents**. You should see the new node agent and its status.

   The node is started as a result of the federation process. If it does not appear to be started in the console, you can check the status from a command window on the node system:

   ```
   cd profile_root\bin
   serverStatus -all
   ```

   If you find that it is not started, start it with this command:

   ```
   cd profile_root\bin
   startNode
   ```

   For more information about managing nodes, see Chapter 6, *Administration of WebSphere processes*.

Creating application servers on the new node: The custom profile does not automatically give you an application server. You can follow the steps in Chapter 6, *Administration of WebSphere processes* to create a new server after the custom profile has been federated to a cell.

Federating an application server profile to a cell

If you are using the administrative console to federate an application server, keep in mind the following considerations:

- Both the deployment manager and the application server must be running.
- You need to be logged into the console with an ID that has administrator privileges.
- The command will connect to the application server. This requires you to specify the application server host name and a user ID that can connect to the server. In turn, the node has to connect to the deployment manager. Specify a user ID and password for this connection.
- You need to specify the host name, JMX™ connection type, and port number to use to connect to the application server. The JMX connection type can be SOAP or RMI. The default is a SOAP connection using port 8880.

To federate an application server profile to a cell (Figure 30), do the following steps:

1. Ensure that the application server and deployment manager are running.
2. Open the deployment manager administrative console.
3. Select **System Administration** → **Nodes** → **Add Node**.
4. Select **Managed node** and click **Next**.
5. Enter the host name and SOAP connector port of the application server profile.

   If you want to keep the sample applications and any other applications you have installed, check the **Include applications** box.

   Enter the administrator user ID and passwords for both the application server and the deployment manager.

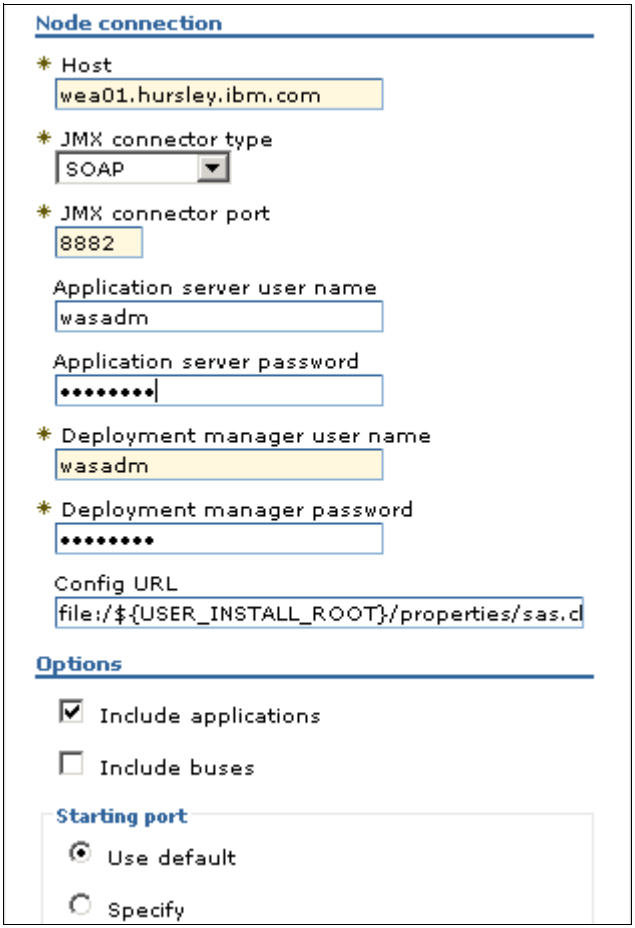

Figure 30 Adding a standalone application profile to a cell

Click **OK**.

6. If the node is a Windows node, you have the opportunity to register the new node agent as a Windows service. Make your selection and click **OK**.

The federation process stops the application server. It creates a new node agent for the node, and adds the node to the cell. The federation process then starts the node agent, but not the server.

You can now display the new node, node agent, and application server from the console. You can also start the server from the console.

At the completion of the process:

- The profile directory for the application server still exists and is used for the new node.
- The old cell name for the application server has been replaced in the profile directory with the cell name of the deployment manager.

  profile_root/config/cells/*dmgr_cell*
- A new entry in the deployment manager profile directory has been added for the new node.

  dmgr_profile_root/config/cells/*dmgr_cell*/nodes/*federated node*
- An entry for each node in the cell is added to the application server profile configuration. Each node entry contains the serverindex.xml file for the node.

  profile_root/config/cells/*dmgr_cell*/nodes/*federated node*

  In turn, an entry for the new node is added to the nodes directory for each node in the cell with a serverindex.xml entry for the new node.

Example 3 shows an example of using the **addNode** command to add an application server profile to a cell. The command specifies the deployment manager host (T60) and the SOAP connector port (8882). Applications currently installed on the application server will still be installed on the server after federation.

Example 3 addNode usage examples

```
C:\WebSphereV7\AppServer\bin>addNode t60 8882 -profileName node40b
-includeapps -username admin -password adminpwd
ADMU0116I: Tool information is being logged in file
           C:\WebSphereV7\AppServer\profiles\node40b\logs\addNode.log
ADMU0128I: Starting tool with the node40b profile
CWPKI0308I: Adding signer alias "default_2" to local keystore
           "ClientDefaultTrustStore" with the following SHA digest:
           9D:99:04:63:97:8C:C0:76:19:46:5A:C4:C0:35:20:FE:DE:21:FD:29
ADMU0001I: Begin federation of node node40b with Deployment Manager at
           t60:8882.
ADMU0009I: Successfully connected to Deployment Manager Server:
t60:8882
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: server40b1
ADMU2010I: Stopping all server processes for node node40b
ADMU0512I: Server server40b1 cannot be reached. It appears to be
stopped.
ADMU0024I: Deleting the old backup directory.
```

```
ADMU0015I: Backing up the original cell repository.
ADMU0012I: Creating Node Agent configuration for node: node40b
ADMU0120I: isclite.ear will not be uploaded since it already exists in
the target repository.
ADMU0120I: DefaultApplication.ear will not be uploaded since it already
exists in the target repository.

ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: node40b
ADMU0020I: Reading configuration for Node Agent process: nodeagent
ADMU0022I: Node Agent launched. Waiting for initialization status.
ADMU0030I: Node Agent initialization completed successfully. Process id
is: 5512
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: nodeagent
ADMU0506I: Server name: server40b1

ADMU0308I: The node node40b and associated applications were
successfully added to the Cell40 cell.

ADMU0306I: Note:
ADMU0302I: Any cell-level documents from the standalone Cell40
configuration have not been migrated to the new cell.
ADMU0307I: You might want to:
ADMU0303I: Update the configuration on the Cell40 Deployment Manager
with values from the old cell-level documents.

ADMU0003I: Node node40b has been successfully federated.
```

Creating an administrative agent profile

This section takes you through the steps of creating an administrative agent profile (Figure 31). Follow these steps:

1. Start the PMT and click the **Launch Profile Management Tool** button on the Welcome page.
2. Click **Create**.
3. Select **Management**. Click **Next**.
4. Select **Administrative agent** and click **Next**.

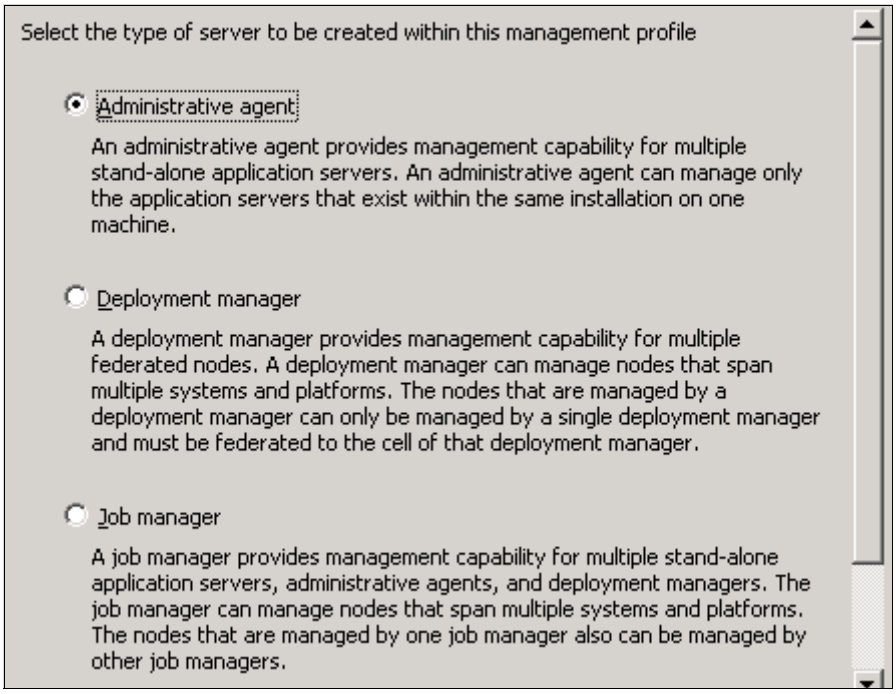

Figure 31 Administrative agent option

5. Select the typical or advanced path. Click **Next**.

   If **Typical** is selected, you only see one more option (to enable security).

   If **Advanced** is selected, you see the next step.

6. Select the option to install the administrative console (Figure 32). Click **Next**.

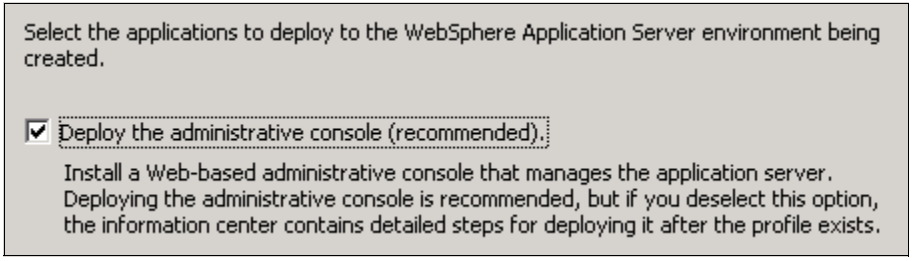

Figure 32 Deploy administrative console

7. Enter a unique name for the profile or accept the default. The profile name becomes the directory name for the profile.

   Click the box if you want this directory to be the default profile for receiving commands (Figure 33). Click **Next**.

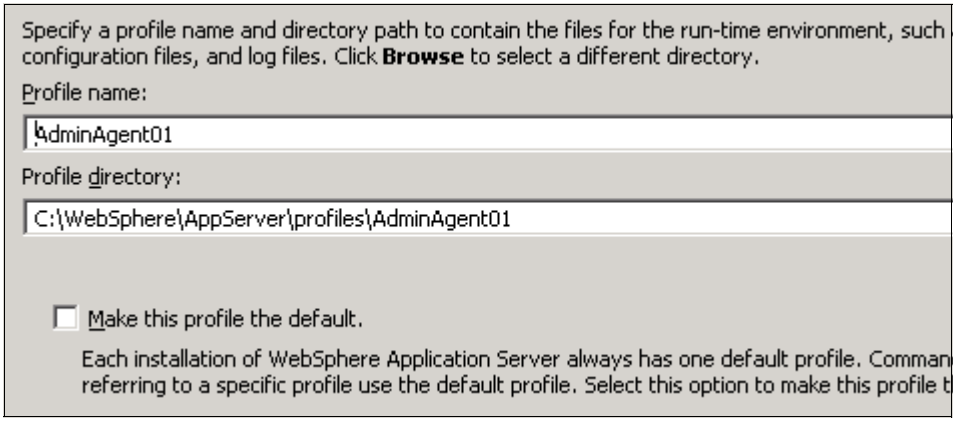

Figure 33 Enter name and location of profile

8. Enter the new node name and the system host name. The node name defaults to the host name of your system. The wizard recognizes if there are existing nodes in the installation and takes this into account when creating the default node name (Figure 34). Click **Next**.

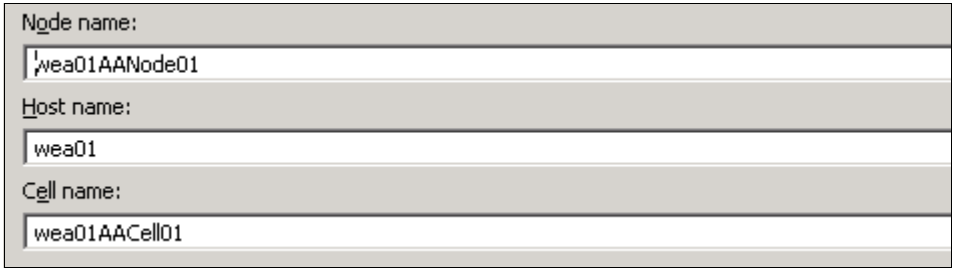

Figure 34 Enter host and node names

9. Choose whether to enable administrative security. If you enable security here, you are asked for a user ID and password that will be added to a file-based user registry with the Administrative role. Click **Next**.
10. Elect to either create new default personal and root signing certificates or to import them. Click **Next**.
11. Review and modify the certificate information as needed. Click **Next**.

12. The wizard presents a list of TCP/IP ports for use by the application server. If you already have existing profiles on the system (within this installation), this will be taken into account when the wizard selects the port assignments, but you should verify that these ports will be unique on the system and alter them if required (Figure 35). Click **Next.**

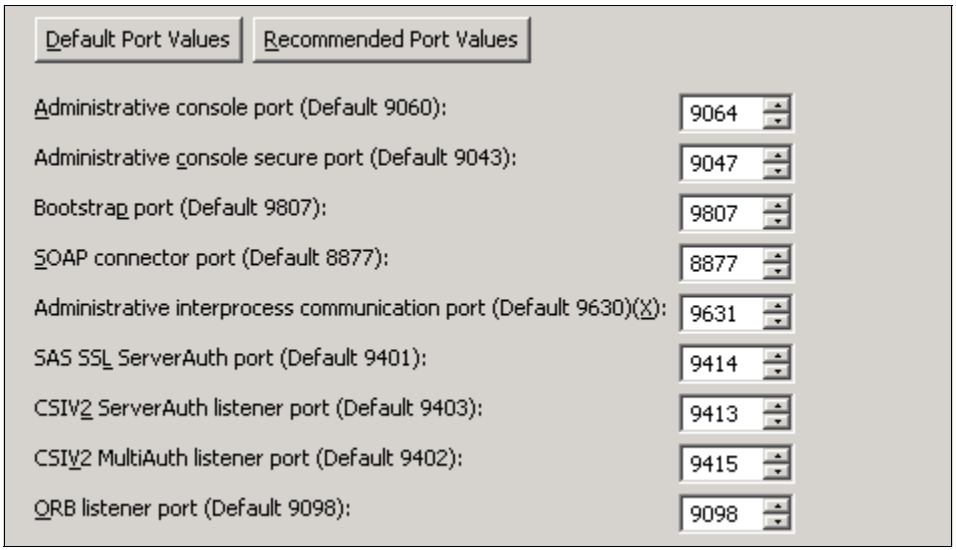

Figure 35 Select ports

Note the administrative console and SOAP connector ports for future use.

13. On Windows systems, select whether to run the administrative agent process as a Windows service.

    Click **Next**.

14. Review the options you have chosen and click **Next** to create the profile.

15. After the wizard has finished, you are presented with the window indicating the success or failure of the process.

    If you have errors, check the log at:

    install_root/logs/manageprofiles/*profile_name*_create.log

    You can also find logs for individual actions stored in:

    profile_root/logs

16. Click **Finish** to close the wizard and start the First Steps application.

17. Run the IVT tests to ensure the installation was successful. The test will start the administrative agent.

18. Open the administrative agent console from the First Steps menu, or using the following URL:

    `http://admin_host:port/ibm/console/`

    Where *port* is the administrative console port selected during profile creation.

19. View the administrative agent by selecting **System Administration** → **Administrative agent** (Figure 36).

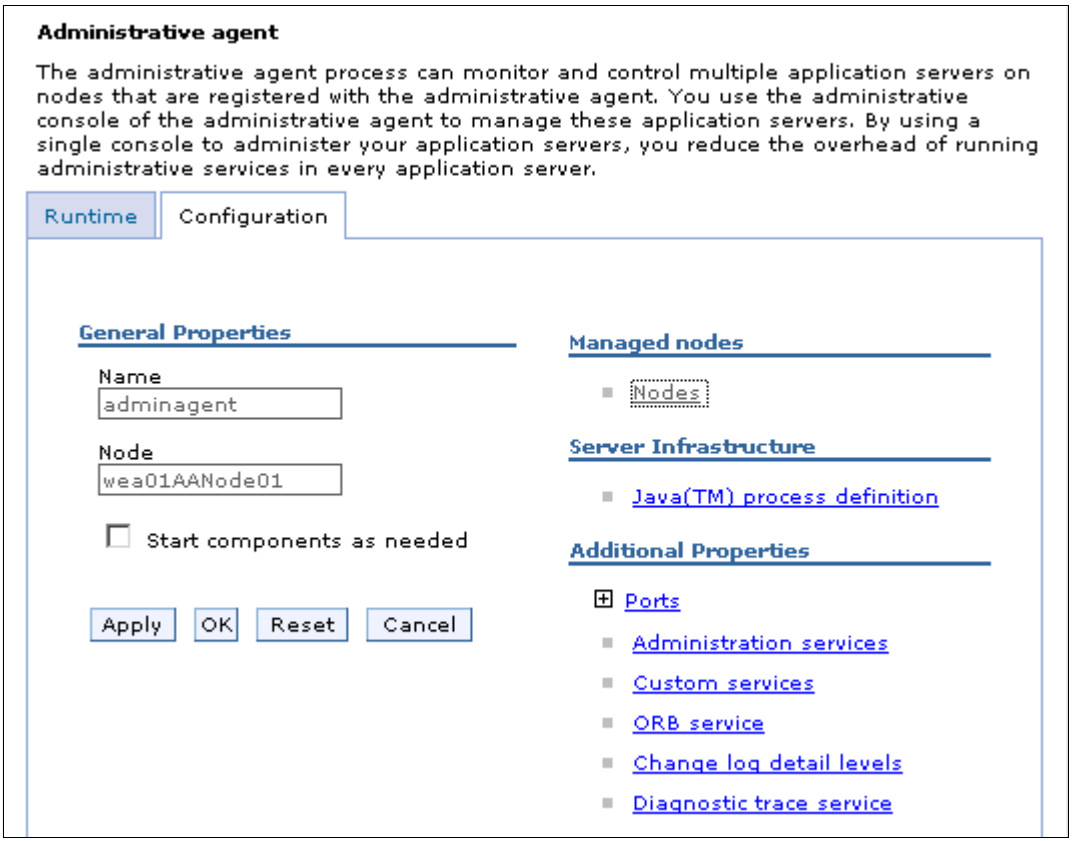

Figure 36 Administrative agent details in the Administration Console

Nodes that are registered to the administrative agent can be viewed by clicking on the **Nodes** link under Managed nodes. The list is initially empty. To register standalone application server nodes to the administrative agent, see “Registering nodes to an administrative agent” on page 53.

Creating a job manager profile

The steps for creating a job manager profile are exactly the same as those for the administrative agent profile:

1. Start the Profile Management Tool and click the **Launch Profile Management Tool** button on the Welcome page.
2. Click **Create**.
3. Select **Management**. Click **Next**.
4. Select **Job manager** and click **Next**.

All further steps are exactly as described in the administrative agent profile.

You can open the job manager console from the First Steps menu, or by using the following URL:

`http://job_manager_host:port/ibm/console/`

Where *port* is the administrative console port selected during profile creation.

Registering nodes to an administrative agent

An administrative agent provides a single interface to unfederated application server nodes (standalone application server profiles).

Notes for use:

- The administrative agent and application servers must be on the same machine or sysplex.
- The administrative agent must be started before running the registerNode command.
- You can only run the command on an unfederated standalone application server. When you run the command, the node for the standalone server is converted into a node that the administrative agent manages.

The **registerNode** command is used to register a node with an administrative agent. The syntax of the command is:

```
registerNode [options]
```

The options can be displayed using the -help parameter (Example 4).

Example 4 registerNode options

```
C:\WebSphereV7\AppServer\bin>registerNode -help
Usage: registerNode -profilePath <path to the base profile to be
registered>

[-host <adminagent host>] [-connType <SOAP | RMI | JSR160RMI | IPC>]
[-port <adminagent JMX port>] [-name <managed node name>]
[-openConnectors <SOAP,IPC,...>] [-username <adminagent user name>]
[-password <adminagent password>] [-nodeusername <base node user name>]
[-nodepassword <base node password>] [-profileName <adminagent profile
name>] [-portsFile <jmx ports filename>] [-trace] [-help]
```

For details on this command, see:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/ragt_registerNode.html

You can enter the command directly. For example, to register the application server defined by the SASrv40 profile to the administrative agent adminAgnt40, you enter the following command:

```
registerNode.bat -profileName adminAgnt40 -profilePath
"C:\WebSphereV7\AppServer\profiles\SASrv40" -host t60 -conntype SOAP
-port 8878 -username admin -password admin
```

Alternatively, you can create an execution file with the **registerNode** command. For example:

1. Create a file with contents similar to Example 5. The name of the file in this example is registerAppSrv03WithAdminAgent.bat. Modify the set statements to match your environment.

Example 5 Sample registerNode bat file contents

```
echo on
set WAS_HOME=C:\WebSphere\AppServer
set appAdminUser=wasadm
set appAdminPassword=wasadm11
set adminAgentAdminUser=wasadm
set adminAgentAdminPassword=wasadm11
set adminAgentProfileName=AdminAgent01
set adminAgentHostName=localhost
set adminAgentSoapPort=8877
set baseProfileName=AppSrv03
```

```
cd %WAS_HOME%\profiles\%adminAgentProfileName%\bin

registerNode.bat -profileName %adminAgentProfileName% -profilePath
"%WAS_HOME%\profiles\%baseProfileName%" -host %adminAgentHostName% -conntype SOAP
-port %adminAgentSoapPort% -username %adminAgentAdminUser% -password
%adminAgentAdminPassword% -nodeusername %appAdminUser% -nodepassword
%appAdminPassword%
```

2. Copy this file to the *adminAgnt_profile_root*/bin directory and run the file. You can see results similar to Example 6. Check the final message to make sure that the node was registered.

Example 6 Sample execution to register a node to the Administration profile

```
echo on

set WAS_HOME=C:\WebSphere\AppServer
set appAdminUser=wasadm
set appAdminPassword=wasadm11
set adminAgentAdminUser=wasadm
set adminAgentAdminPassword=wasadm11
set adminAgentProfileName=AdminAgent01
set adminAgentHostName=localhost
set adminAgentSoapPort=8877
set baseProfileName=AppSrv03

registerNode.bat -profileName AdminAgent01 -profilePath
"C:\WebSphere\AppServer\profiles\AppSrv03" -host localhost -conntype SOAP -port 8877
-username wasadm -password wasadm11 -nodeusername wasadm -nodepassword wasadm11
ADMU0116I: Tool information is being logged in file
           C:\WebSphere\AppServer\profiles\AdminAgent01\logs\registerNode.log
ADMU0128I: Starting tool with the AdminAgent01 profile
ADMU8053I: Successfully connected to AdminAgent Server: localhost:8877
ADMU8002I: Exchanging signers between adminagent and node with path
           C:\WebSphere\AppServer\profiles\AppSrv03.
ADMU8007I: Exchanged signers successfully.
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: server1
ADMU2010I: Stopping all server processes for node wea01Node03
ADMU0512I: Server server1 cannot be reached. It appears to be stopped.
ADMU8010I: Begin registration of Application Server with path
           C:\WebSphere\AppServer\profiles\AppSrv03
ADMU0024I: Deleting the old backup directory.
ADMU8004I: Backing up the original config directory of the node will be
           registered.
```

```
ADMU8037I: Backing up the original wsadmin.properties file of the node will be
           registered.
ADMU8036I: Registering the node with an AdminAgent.
ADMU8042I: Node has been successfully registered.
ADMU8040I: The administrative agent is initializing the administrative
           subsystem for the registered node.
ADMU8014I: The administrative subsystem for registered node has been
           successfully initialized.
ADMU8041I: The administrative agent is starting the administrative subsystem
           for the registered node.
ADMU8015I: The administrative subsystem for registered node has been
           successfully started.
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: server1
ADMU8012I: Application Server with path
           C:\WebSphere\AppServer\profiles\AppSrv03 has been successfully
           registered.
```

3. The next time you log on to the administrative agent console, you have the option to select a node to administer. In this case, you can select between the administrative agent (the top choice) and the new node you registered.

   Select the administrative agent to view the new configuration (Figure 37).

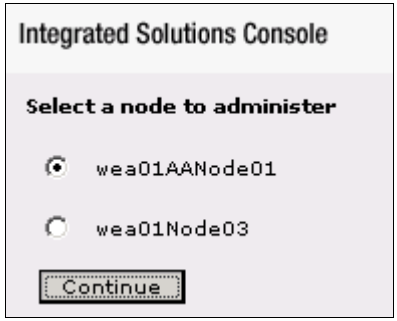

Figure 37 Option to pick which local Application Server to administer

4. Select **System Administration** → **Administrative agent** → **Nodes**. This shows that this node is now registered with the administrative agent (Figure 38).

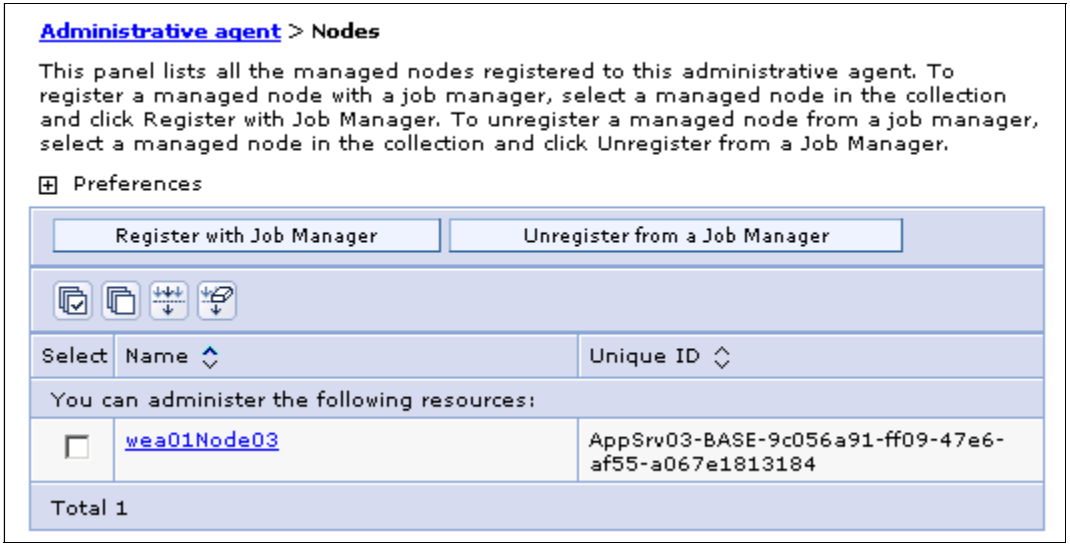

Figure 38 Node registered with administrative agent

Deregistering a node from the administrative agent

To deregister a node from the administrative agent, use the **deregisterNode** command (Example 7). Run this command from the *adminAgnt_profile_root*/bin directory.

Example 7 deRegisterNode command

```
deregisterNode.bat -connType SOAP -port 8877 -profilePath
C:\WebSphere\AppServer\profiles\AppSrv03 -username wasadm -password wasadm11
```

Registering an administrative agent node with a job manager

This section describes the steps to register nodes within the administrative agent with a job manager:

1. Log on to the administrative agent node (Figure 39).

Figure 39 Option to pick which local Application Server to administer

Navigate to **System administration** → **Administrative agent** (Figure 40).

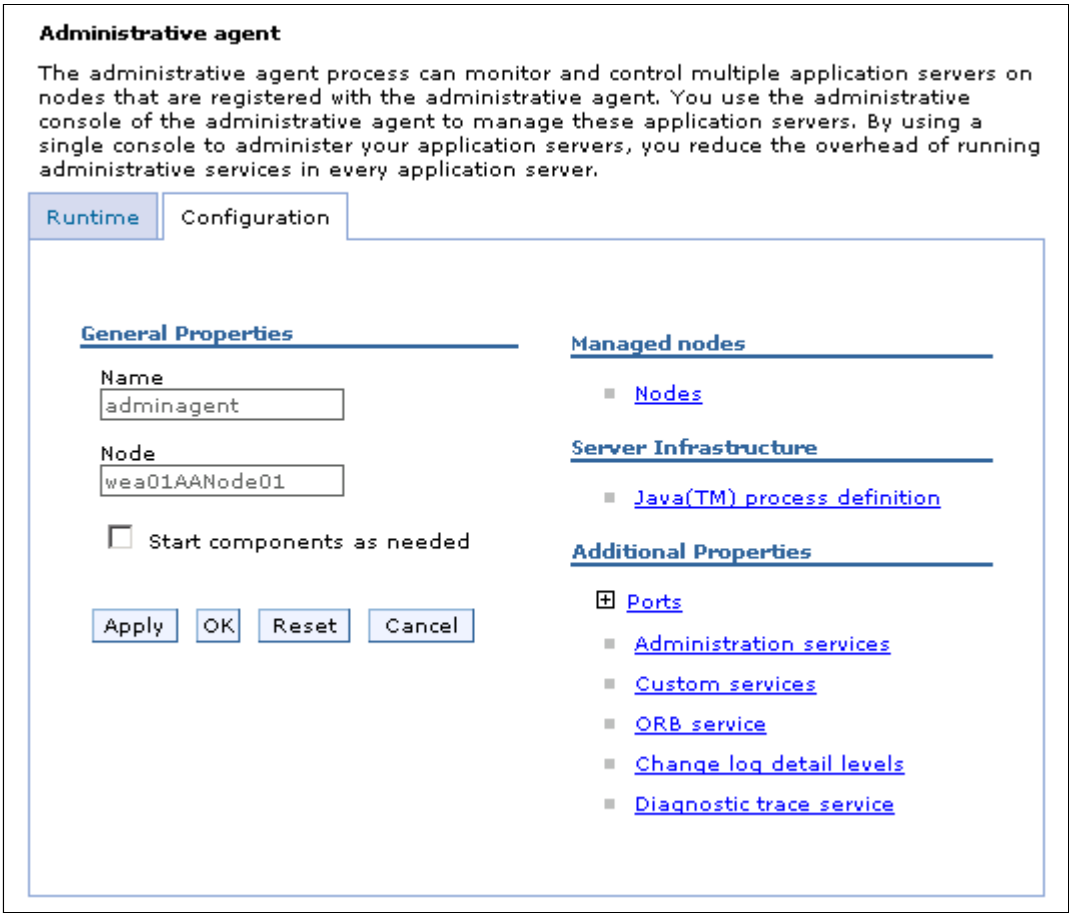

Figure 40 Administrative agent details

2. Click **Nodes** and select the node that you want to register with the job manager (Figure 41).

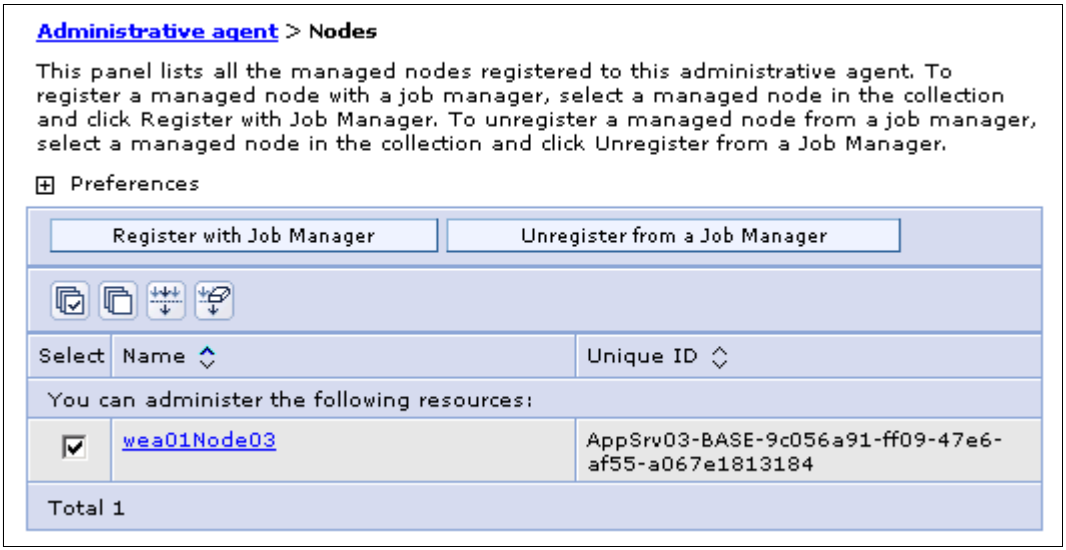

Figure 41 Select which node will be registered with the job manager

Note: You can register some or all of the nodes with the job manager. Or you can register some nodes with one job manager and other nodes with another job manager.

Click **Register with Job Manager**.

3. Enter the information required to connect to the job manager, including the host name, administrative host port, and user ID and password.

   If the node name you are registering is already in use by the job manager, you can enter an alias for the node (Figure 42).

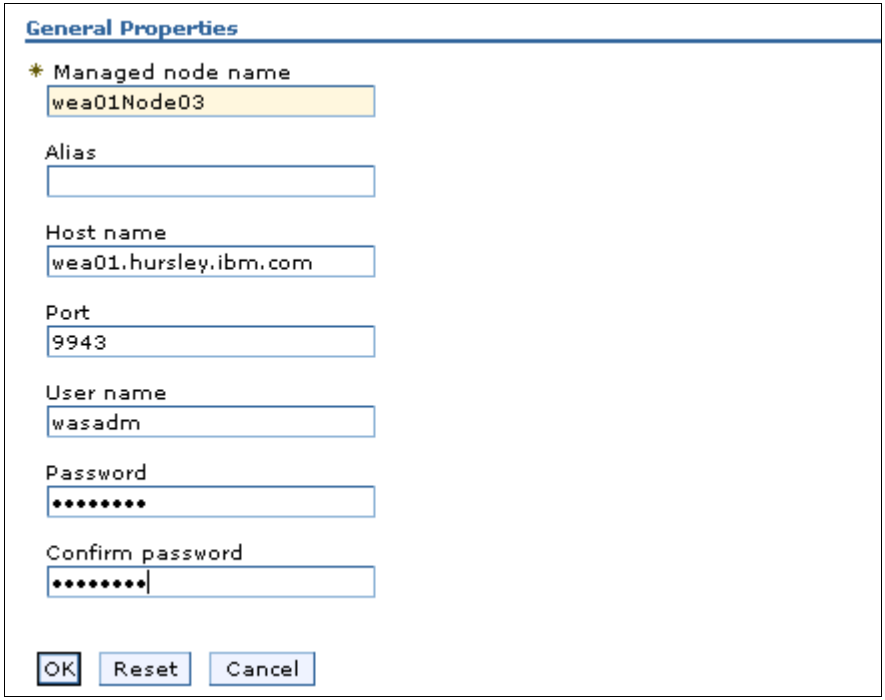

Figure 42 Detailed options for registering a node with a job manager

Click **OK** to register the node.

4. Log in to the job manager and go to **Jobs** → **Nodes** to see the newly registered node (Figure 43).

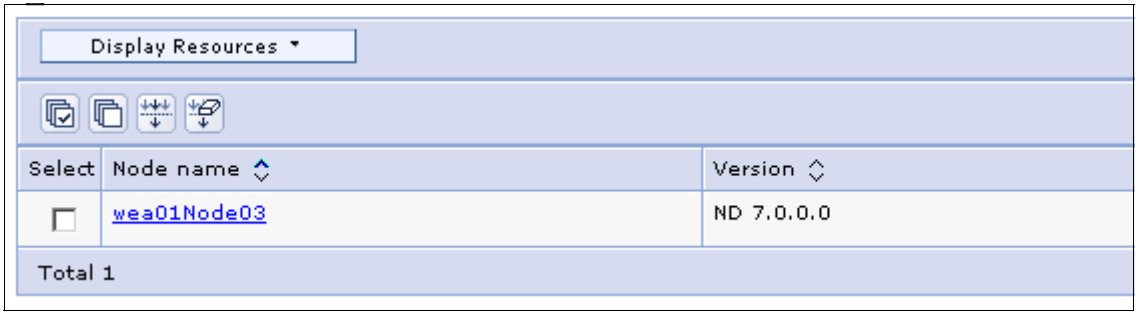

Figure 43 Nodes that the job manager is able to administer

For equivalent command line steps for this process, see the IBM InfoCenter at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.nd.doc/info/ae/ae/txml_7regmannode.htm

Registering a deployment manager with a job manager

This section describes the steps to register a deployment manager node with a job manager:

1. Log in to the deployment manager administrative console and go to **System Environment** → **Deployment Manager**.
2. Under Additional Properties, select **Job managers**.
3. Click the **Register with Job Manager** button (Figure 44).

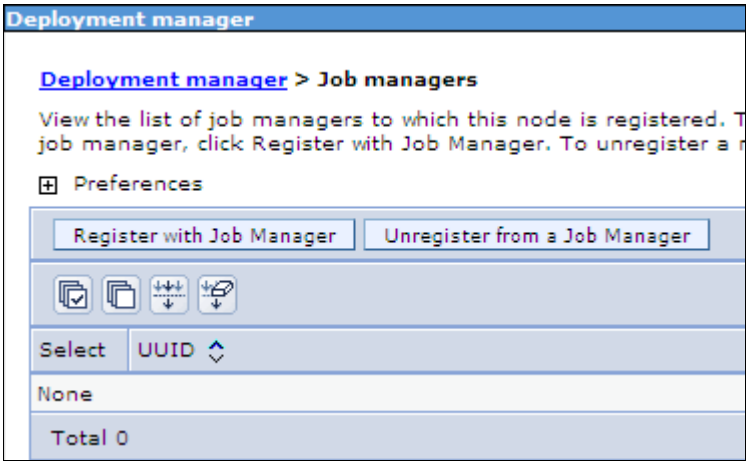

Figure 44 Registering a deployment manager with a job manager

4. Enter the information required to connect to the job manager, including the host name, administrative host port, and user ID and password.

   If the node name you are registering is already in use by the job manager, you can enter an alias for the node.

   Click **OK** (Figure 45).

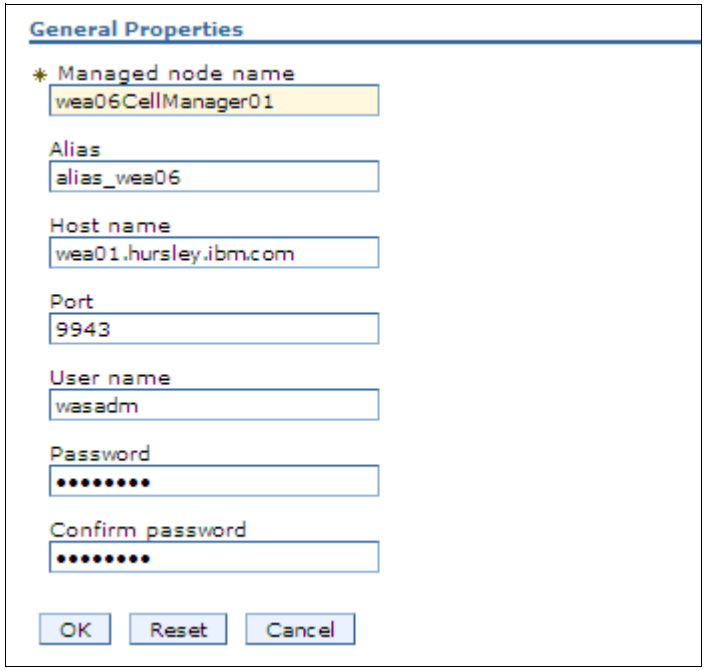

Figure 45 Job manager details

This registers the deployment manager with the job manager.

5. To view the newly registered deployment manager, log in to the job manager console and select **Jobs** → **Nodes**. This lists the nodes and deployment managers that are registered with the job manager (Figure 46).

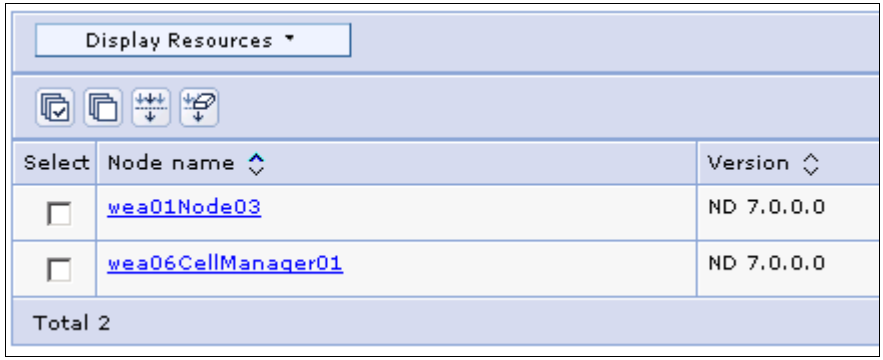

Figure 46 Nodes that the job manager can administer

Managing profiles

Each profile you create is registered in a profile registry:

install_root/properties/profileRegistry.xml

You have already seen how profiles are created with the Profile Management Tool. At the heart of this wizard is the **manageprofiles** command. This command provides you with the means to do normal maintenance activities for profiles. For example, you can call this command to create profiles natively or silently, list profiles, delete profiles, validate the profile registry, and other functions.

Using the manageprofiles command

The **manageprofiles** command can be found in the *install_root*/bin directory.

The syntax is:

- manageprofiles(.sh) -mode -arguments

The modes listed in Table 3 are available.

Table 3 manageprofiles modes

Mode	Use
-create	Creates a new profile.
-delete	Deletes a profile
-augment	Augments the given profile using the given profile template
-unaugment	Unaugments the profile
-unaugmentAll	Unaugments all the profile
-deleteAll	Deletes all registered profiles.
-listProfiles	Lists the profiles in the profile registry.
-listAugments	Lists the registered augments on a profile that is in the profile registry
-getName	Returns the name of the profile at the path specified.
-getPath	Returns the path of the profile name specified.
-validateRegistry	Validates the profile registry and returns a list of profiles that are not valid
-validateAndUpdateRegistry	Validates the profile registry and lists the non-valid profiles that it purges

Mode	Use
-getDefaultName	Returns the name of the default profile.
-setDefaultName	Sets the default profile.
-backupProfile	Back ups the given profile into a zip file.
-restoreProfile	Restores the given profile from a zip file.
-response	Manage profiles from a response file
-help	Shows help.

Getting help

Enter **manageprofiles *-mode* -help** for detailed help on each mode. Example 8 shows the help information for the -create mode.

Example 8 Getting help for the manageprofiles command

```
C:\WebSphere\AppServer\bin>manageprofiles -create -help
Function: Creates a new profile

Syntax:
manageprofiles -create -<argument> <argument parameter> ...

Arguments:
The following command line arguments are required for this mode:
-templatePath <argument parameter>: The fully qualified pathname of the
profile template that is located on the file system.
-profileName <argument parameter>: The name of the profile.
-profilePath <argument parameter>: The intended location of the profile
in the file system.

The following command line arguments are optional, and have no default
values:
-isDefault <argument parameter>: Make this profile the default target
of commands that do not use their profile parameter.
-omitAction <argument parameter>: Omit optional features.

Note: Command-line arguments are case sensitive.
   Note: If argument accepts a parameter containing spaces, the
parameter must be enclosed in "double quotes".
   Note: The default profile template is "default" and may be
overridden by the -templatePath switch.
```

```
   Note: Each profile template will have its own set of required and
optional arguments.
```

Getting a list of profiles

Enter **manageprofiles -listProfiles** to see a list of the profiles in the registry. Example 9 shows a sample output of -listProfiles.

Example 9 Listing profiles

```
C:\WebSphere\AppServer\bin>manageprofiles -listProfiles
[AppSrv01, Dmgr01, Custom01, AppSrv02, AdminAgent01, JobMgr01,
AppSrv03]
```

Depending on the operation used, there will be other parameters that are required. These other parameters are documented in the Information Center. To find the relevant articles, search for “manageprofile”.

Creating a profile with the manageprofiles command

You can use the **manageprofiles** command to create profiles.

Profile templates

Profiles are created based on templates supplied with the product. These templates are located in *install_root*/profileTemplates. Each template consists of a set of files that provide the initial settings for the profile and a list of actions to perform after the profile is created. When you create a profile using **manageprofiles**, you need to specify one of the following templates:

- Default (for application server profiles)
- Management (for deployment manager, job manager, and administrative agent profiles)
- Managed (for custom profiles)
- Cell (for cell profiles)

For example, the command used to create a deployment manager with node name TestDmgr01 under profile name TestDmgr01 is shown in Figure 10.

Example 10 Creating a profile with the manageprofiles command

```
manageprofiles.bat -create -templatePath
c:/WebSphere /AppServer/profileTemplates/management -serverType
DEPLOYMENT_MANAGER -profileName TestDmgr01 -profilePath
```

```
c:/WebSphere/AppServer/profiles/TestDmgr01 -enableAdminSecurity true
-adminUserName wasadmin -adminPassword wasadmin11 -cellName TestCell01
-nodeName TestDmgr01
```

Log files that result when you run the manageprofiles command are located in:

install_root/logs/manageprofile/*profilename_action*.log

For example:

C:/WebSphere/AppServer/logs/manageprofiles/TestDmgr01_create.log

Additional log files are created in:

install_root/logs/manageprofile/*profile_name*/

For example:

C:/WebSphere/AppServer/logs/manageprofiles/TestDmgr01

Important: Do not manually modify the files that are located in the *install_root*/ profileTemplates directory.

Options for specifying ports

During profile creation using the **manageprofiles** command, you can accept the default port values, or you can specify your port settings. If you want to specify ports, you can do so in any of the following ways:

- Specify the use of a port file that contains the port values.
- Specify the use of a starting port value.
- Specify the use of the default port values.

Port file that contains the port values

You can supply a file containing the port values that you want to use for any profile using the -portsFile option. See Example 11 for an example ports file named portdef.props.

Example 11 Example contents of portdef.props file

```
WC_defaulthost=39080 WC_adminhost=39060 WC_defaulthost_secure=39443
WC_adminhost_secure=39043 BOOTSTRAP_ADDRESS=32809 SOAP_CONNECTOR_ADDRESS=38880
IPC_CONNECTOR_ADDRESS=39633 SAS_SSL_SERVERAUTH_LISTENER_ADDRESS=39401
CSIV2_SSL_SERVERAUTH_LISTENER_ADDRESS=39403
CSIV2_SSL_MUTUALAUTH_LISTENER_ADDRESS=39402 ORB_LISTENER_ADDRESS=39100
DCS_UNICAST_ADDRESS=39353 SIB_ENDPOINT_ADDRESS=37276
SIB_ENDPOINT_SECURE_ADDRESS=37286 SIB_MQ_ENDPOINT_ADDRESS=35558
SIB_MQ_ENDPOINT_SECURE_ADDRESS=35578 SIP_DEFAULTHOST=35060
SIP_DEFAULTHOST_SECURE=35061
```

Incrementing port numbers from a starting point

The **manageprofiles** command can assign port numbers based on a starting port value. You can provide the starting port value from the command line, using the -startingPort parameter. The command assigns port numbers sequentially from the starting port number value. However, if a port value in the sequence conflicts with an existing port assignment, the next available port value is used.

The order of port assignments is arbitrary. Predicting assignments is not possible.

Use the **-startPort** option for the **manageprofiles** command.

Default ports

This option assigns the default or base port values to the profile. Use the *-defaultPorts* option to the **manageprofile** command.

Changing port settings after profile creation

Use the **updatePorts** tool to change port settings.

For more information, read the article, “Updating ports in an existing profile,” at:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.installation.nd.doc/info/ae/ae/tins_updatePorts.html

Creating a profile in silent mode with PMT

Profiles can also be created in silent mode using a response file. The command to use is:

```
pmt(.sh) -options response_file -silent
```

The command to start the wizard is platform-specific and is located in *install_root*/bin/ProfileManagement.

Deleting profiles

To delete a profile, do the following actions:

- If you are removing a custom profile or application server profile that has been federated to a cell:
  - Stop the application servers on the node.
  - Remove the node from the cell using the administrative console or the **removeNode** command. Removing a node does not delete it, but restores it to its pre-federated configuration that was saved as part of the federation process.
  - Delete the profile using **manageprofiles -delete -profileName** *profile_name*.
  - Use the **manageprofiles -validateAndUpdateRegistry** command to clean the profile registry.
  - Delete the *profile_root* directory.
- If you are removing an application server profile that has not been federated to a cell:
  - Stop the application server.
  - Delete the profile using **manageprofiles -delete -profileName** *profile_name*
  - Use the **manageprofiles -validateAndUpdateRegistry** command to clean up the profile registry.
  - Delete the *profile_root* directory.
- If you are removing a deployment manager profile:
  - Remove any nodes federated to the cell using the administrative console or the **removeNode** command. Removing a node does not delete it, but restores it to its pre-federated configuration that was saved as part of the federation process.
  - Stop the deployment manager.
  - Delete the profile using **manageprofiles -delete -profileName** *profile_name*.
  - Use the **manageprofiles -validateAndUpdateRegistry** command to clean the profile registry.
  - Delete the *profile_root* directory.

If you have errors while deleting the profile, check the following log:

install_root/logs/manageprofile/*profilename*_delete.log

For example, in Example 12, you can see the use of the **manageprofiles** command to delete the profile named Node06.

Example 12 Deleting a profile using manageprofiles

```
C:\WebSphere\ND\profiles\Dmgr01\bin>manageprofiles -delete -profileName
Node06
INSTCONFSUCCESS: Success: The profile no longer exists.
```

As you can see, all seems to have gone well. But, as an additional step to ensure the registry was properly updated, you can list the profiles to ensure that the profile is gone from the registry, and validate the registry. See Example 13.

Example 13 Verifying the delete profile results

```
C:\WebSphere\ND\profiles\Dmgr01\bin>manageprofiles -listProfiles
[Dmgr01, AppSrv01, AppSrv02, SamplesServer, WebServer2Node, DmgrSecure]

C:\WebSphere\ND\profiles\Dmgr01\bin> manageprofiles
-validateAndUpdateRegistry
[]
```

Note: If there are problems during the delete, you can manually delete the profile. For information about this, see the topic, *Deleting a profile*, in the Information Center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tpro_removeprofile.html

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.

This document REDP-4570-00 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