



Getting started with the Feature Pack for Service Component Architecture (SCA) Version 1.0

Note

Before using this information, be sure to read the general information under Appendix A, "Notices," on page 239.

Compilation date: December 3, 2009

© Copyright International Business Machines Corporation 2009.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Chapter 1. Supported operating systems 1

Chapter 2. Installing the Feature Pack for SCA Version 1.0 on distributed operating systems 3

| | |
|---|---|
| Installing the Feature Pack for SCA Version 1.0 silently on distributed operating systems | 6 |
| Uninstalling the Feature Pack for SCA on distributed operating systems | 9 |

Chapter 3. Installing the Feature Pack for SCA Version 1.0 on IBM i systems . 13

| | |
|---|----|
| Uninstalling the Feature Pack for SCA on IBM i systems. | 15 |
|---|----|

Chapter 4. Installing the Feature Pack for SCA Version 1.0 on z/OS systems . 17

| | |
|---|----|
| Augmentation rules and limitations for feature packs on z/OS | 19 |
| Configuring with the Profile Management Tool | 22 |
| Using the Profile Management Tool to create z/OS standalone application servers with the Feature Pack for SCA installed | 23 |
| Using the Profile Management Tool to enable existing z/OS standalone application servers for the Feature Pack for SCA. | 33 |
| Using the Profile Management Tool to create z/OS deployment managers with the Feature Pack for SCA installed. | 36 |
| Using the Profile Management Tool to enable existing z/OS deployment managers for the Feature Pack for SCA | 46 |
| Using the Profile Management Tool to create z/OS managed (custom) nodes with the Feature Pack for SCA installed. | 49 |
| Using the Profile Management Tool to enable existing z/OS managed (custom) nodes for the Feature Pack for SCA | 58 |
| Using the Profile Management Tool to create z/OS Network Deployment cells with the Feature Pack for SCA installed | 61 |
| Configuring with the zpm command | 73 |
| zpm command | 75 |
| Variables for using the zpm command to create z/OS standalone application servers with the feature pack installed | 77 |
| Variables for using the zpm command to enable existing z/OS standalone application servers for the feature pack | 90 |
| Variables for using the zpm command to create z/OS deployment managers with the feature pack installed. | 92 |

| | |
|--|-----|
| Variables for using the zpm command to enable existing z/OS deployment managers for the feature pack | 103 |
| Variables for using the zpm command to create z/OS managed (custom) nodes with the feature pack installed | 106 |
| Variables for using the zpm command to enable existing z/OS managed (custom) nodes for the feature pack | 116 |
| Variables for using the zpm command to create z/OS Network Deployment cells with the feature pack installed. | 119 |
| Applying maintenance to the Feature Pack for SCA on z/OS systems | 136 |

Chapter 5. Managing profiles on non-z/OS operating systems 139

| | |
|--|-----|
| Profile concepts | 140 |
| Profiles: File-system requirements | 148 |
| Augmentation rules and limitations for feature packs on non-z/OS operating systems | 150 |
| Managing profiles using commands | 153 |
| Creating profiles enabled for a feature pack using the command prompt | 155 |
| Augmenting a profile using the command prompt | 156 |
| Unaugmenting a profile using the command prompt | 158 |
| Managing profiles using the graphical user interface | 159 |
| Creating management profiles with deployment managers. | 161 |
| Creating management profiles with administrative agents. | 169 |
| Creating management profiles for job managers | 177 |
| Creating secure proxy profiles. | 186 |
| Creating cell profiles | 194 |
| Creating custom profiles. | 203 |
| Creating application server profiles | 211 |
| Augmenting profiles using the graphical user interface | 219 |
| Managing profiles for non-root users | 221 |
| Assigning profile ownership to a non-root user | 222 |
| Granting write permission for profile-related tasks | 224 |
| Changing ownership for profile maintenance | 227 |
| Deleting profiles | 228 |

Chapter 6. Directory conventions . . . 231

Appendix A. Notices 239

Appendix B. Trademarks and service marks. 241

Chapter 1. Supported operating systems

All versions of the Feature Pack for Service Component Architecture (SCA) are supported on the AIX[®], HP-UX, Linux[®], Solaris, Windows[®], and z/OS[®] operating systems. The subject of this guide, Feature Pack for SCA Version 1.0, is the only version of the feature pack that is supported on the IBM[®] i operating system. Feature Pack for SCA Version 1.0.1 and later are not supported on the IBM i operating system.

Chapter 2. Installing the Feature Pack for SCA Version 1.0 on distributed operating systems

Run the Feature Pack for Service Component Architecture (SCA) installation program to install this version of feature pack on an existing installation of a WebSphere® Application Server Version 7.0 product. The Feature Pack for SCA is an optionally installable product extension for WebSphere Application Server that delivers an integrated, open implementation of SCA technology specified by IBM and other industry leaders through the Open SOA Collaboration.

Before you begin

Before starting this installation, do the following:

1. Install a WebSphere Application Server Version 7.0 product if you have not done so already.

2. Download and extract the Feature Pack for SCA.

For example, create two directories, `sca_download` and `sca_installation_image`. Download the feature pack to the `sca_download` directory and then extract the downloaded file to the `sca_installation_image` directory. Do not move any files from the `sca_installation_image` directory.

3. The operating system requirements for a feature pack are the same as for the application server installation. However, you need to ensure that you have enough free disk space to install the feature pack onto the application server installation. The following disk space is required:

- 1800 MB of free space available in your target installation directory. This estimate includes the application server maintenance bundled with the feature pack and is in addition to the existing application server product.
- 600 MB of free space available in your temporary directory

Note: You must have the application server samples installed to use the SCA samples. If you did not install the application server samples, then remove any fixes or fix packs you have applied to the application server, run the application server installer, and add the samples to your application server. Reinstall the fixes or fix packs.

About this task

Install the SCA feature pack using the installation wizard. To install the feature pack silently, read the “Installing the Feature Pack for SCA Version 1.0 silently on distributed operating systems” on page 6 topic.

The installation program installs the following program files if they are not already installed:

- WebSphere Application Server Version 7.0 Fix Pack 1
- Java SDK 1.6 Cumulative Fix for WebSphere Application Server
- WebSphere Application Server Version 7.0 Feature Pack for SCA Version 1.0

Consider your current product topography before installing the feature pack because it installs maintenance packages that might affect the version of your application server product. If the application server is already at or above the

levels of maintenance included with the feature pack, then the maintenance packages are not installed.

1. Log on to the system.
 - **AIX** **HP-UX** **Linux** **Solaris** Log on using the same user ID that was used when the product was installed or as a user who has write permissions to *app_server_root*.
Run the `ls -al` command at the root of the application server installation to find the user ID that was used to install the product.
 - **Windows** Log on as a user who belongs to the administrator group or as a user who has write permissions to *app_server_root*
2. Stop all processes for the application server product on which you are installing the feature pack.
Stop the application server and any other product processes. For example, for the Network Deployment product, stop the deployment manager, the node agent, and all application server processes.
3. Run the feature-pack installation program.
Run the installation executable from the command line in the SCA directory:
 - **AIX** **HP-UX** **Linux** **Solaris** `./install`
 - **Windows** `install.exe`
4. Complete the steps in the feature-pack installation wizard.
 - a. On the Welcome panel, click **Next**.
 - b. On the Software License Agreement panel, select **I accept the terms in the license agreement** and click **Next**.
 - c. On the System prerequisites check panel, do the following:
 - Read the panel information. The panel informs you whether your machine has a supported operating system with all service packs and patches needed by the feature pack installed.
 - If the system prerequisite check shows **Passed**, click **Next**.
 - If the check shows **Failed**, click **Cancel**. Install operating system service packs and patches needed for the feature pack, and then try installing the feature pack again. Or, click **Next** to continue the installation even though the check shows **Failed**.
 - d. On the Installation Directory panel, specify the location of the *app_server_root* directory of your existing WebSphere Application Server installation and click **Next**. If the specified application server is not at the 7.0.0.1 level, you are asked whether you want the SCA installation to update the application server for you, or whether you want to exit the wizard and apply the 7.0.0.1 fix pack manually.
 - e. On the Maintenance Package Selection panel, optionally specify the location of up to one SCA fix pack and one SCA refresh pack and click **Next**.
 - f. On the Installation Summary panel, click **Next**. The installation program copies feature-pack program files onto your application server installation.
 - g. On the Installation Results panel, click **Finish**.
Keep the **Launch the Profile management tool console** default selection.

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

Results

The installation wizard installs the feature pack and records installation events in the installation log files, which are located in the *app_server_root/logs/sca/install* directory.

Troubleshooting

Examine messages that the installation program displays. If the feature pack does not install successfully, read the messages to identify why the installation failed. Correct the problems identified and try installing the product again.

Note: Certain events can prevent ISMP from starting the installation wizard. Such an event is not enough disk space to launch the installation wizard for example. If your installation fails and there is no information in the installation logs, use the `-is:javaconsole` parameter to record entries for events that cause the ISMP program to fail to start the installation wizard. The syntax of the install command for observing such events is:

```
AIX      HP-UX      Linux      Solaris  
./install -is:javaconsole
```

```
Windows  
install.exe -is:javaconsole
```

Note: Although the usage of `-is:javaconsole` is supported, the usage of `-console`, for example `install -console`, is not supported.

What to do next

To use the feature-pack functionality, you must create a new profile with the feature pack enabled or augment an existing profile with the feature pack.

- **Create a new profile**

You can use the `manageprofiles` command or the Profile Management tool to create a new profile that is enabled to use the feature-pack functionality.

For example, follow these steps to create a profile using the Profile Management tool:

1. Open the Profile Management tool.
2. On the Profile Management Tool panel, click **Create**.
3. On the Welcome to the Profile Management tool panel, click **Next**.
4. On the Environment Selection panel, select one of the available profile types and click **Next**.
5. Complete the steps to create the profile.

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

After you create the profile, start the server and open the administrative console for the application server.

- **Augment an existing profile**

You can run the `manageprofiles` command or the Profile Management tool to augment a profile to use the feature-pack functionality.

For example, to augment an application server profile with SCA functionality using the `manageprofiles`, open a command prompt in the `app_server_root/bin` directory, enter the following command to augment the `AppSrv01` profile:

```
manageprofiles -augment -profileName AppSrv01 -templatePath app_server_root/profileTemplates/SCA/default.scafep
```

After you augment the profile, start the server and open the administrative console for the application server.

Read the profile topics for more information.

Installing the Feature Pack for SCA Version 1.0 silently on distributed operating systems

Run the Feature Pack for Service Component Architecture (SCA) Version 1.0 installation program to silently install the feature pack on an existing installation of a WebSphere Application Server Version 7.0 product. The Feature Pack for SCA is an optionally installable product extension for WebSphere Application Server that delivers an integrated, open implementation of SCA technology specified by IBM and other industry leaders through the Open SOA Collaboration.

Before you begin

Before starting this installation, do the following:

1. Install a WebSphere Application Server Version 7.0 product if you have not done so already.
2. Download and extract the Feature Pack for Service Component Architecture.
For example, create two directories, `sca_download` and `sca_installation_image`. Download the feature pack to the `sca_download` directory and then extract the downloaded file to the `sca_installation_image` directory. Do not move any files from the `sca_installation_image` directory.
3. The operating system requirements for a feature pack are the same as for the application server installation. However, you need to ensure that you have enough free disk space to install the feature pack onto the application server installation. The following disk space is required:
 - 1800 MB of free space available in your target installation directory. This estimate includes the application server maintenance bundled with the feature pack and is in addition to the existing application server product.
 - 600 MB of free space available in your temporary directory

Note: You must have the application server samples installed to use the SCA samples. If you did not install the application server samples, then remove any fixes or fix packs you have applied to the application server, run the application server installer, and add the samples to your application server. Reinstall the fixes or fix packs.

About this task

This topic describes how to install the feature pack silently. To install the feature pack using the installation wizard, read the Chapter 2, “Installing the Feature Pack for SCA Version 1.0 on distributed operating systems,” on page 3 topic.

The installation program installs the following program files if they are not already installed:

- WebSphere Application Server Version 7.0 Fix Pack 1 (7.0.0.1)
- Java SDK 1.6 Cumulative Fix for WebSphere Application Server (7.0.0.1)
- WebSphere Application Server Version 7.0 Feature Pack for SCA

Consider your current product topography before installing the feature pack because it installs maintenance packages that may affect the version of your application server product. If the application server is already at or above the levels of maintenance included with the feature pack, then the installation of these maintenance packages is skipped.

1. Log on to the system.

- **AIX** **HP-UX** **Linux** **Solaris** Log on using the same user ID that was used when the product was installed or as a user who has write permissions to *app_server_root*.

Run the `ls -al` command at the root of the application server installation to find the user ID that was used to install the product.

- **Windows** Log on as a user who belongs to the administrator group or as a user who has write permissions to *app_server_root*

2. Extract the downloaded product files. Make a copy of the `responsefile.SCA.txt` file in the root directory of the feature pack installation image.

3. Edit the response file and customize it for your environment.

Set values for the following options:

Table 1. Feature pack response file options.

Edit and customize the response file for your environment.

| Option | Description |
|--|--|
| <code>-OPT silentInstallLicenseAcceptance="true"</code> | You must accept the enclosed license agreement to install the feature pack. |
| <code>-OPT allowNonRootSilentInstall="true"</code> | You must uncomment this line if you are installing the product with a non-root or non-administrator ID. |
| <code>-OPT installLocation=app_server_root</code> | Set <i>app_server_root</i> to the root directory of your application server product. |
| <code>-OPT checkFilePermissions="true"</code> | Uncomment this option if you want the feature pack installer to verify whether the current user has permission to write to the specified directories and files. |
| <code>-OPT disableNonBlockingPrereqChecking="true"</code> | Uncomment this option in order to install application server and SDK fix packs, if they are required. The installer will fail if you have not uncommented this option and your application server still requires the fix packs bundled with the feature pack. Uncomment this line to notify the installer to continue with the installation and log the warnings even though prerequisite checking failed. |
| <code>-OPT fepRefreshpackLocation="<refresh_pack_location_and_file_name>"</code> | The feature pack installer is capable of applying refresh packs and fix packs for the WebSphere Application Server v7.0 Feature Pack for SCA. However, applying higher level feature pack maintenance during installation is optional. Specify the directory paths and file names of the feature pack maintenance packages to apply during installation. Otherwise, leave these options commented out. |
| <code>-OPT fepFixpackLocation="<fix_pack_location_and_file_name>"</code> | |

4. If the feature pack is installed on a Network Deployment product, perform the following tasks:

- a. Stop the node agent process that might be running on the system.

For example, issue the following command from the *profile_root/bin* directory of a federated node on a Linux workstation to stop the node agent process:

```
./stopNode.sh
```

If servers are running and security is enabled, then use the following command:

```
./stopNode.sh -user user_ID -password password
```

- b. Stop the deployment manager dmgr process.

For example, issue the following command on a Linux workstation from the *profile_root/bin* directory of the deployment manager profile:

```
./stopManager.sh -user user_ID -password password
```

5. Stop each running application server.

Stop all server processes in all profiles associated with the target product instance. For example, issue the following command from the *profile_root/bin* directory to stop the server1 process in the application server profile:

```
AIX HP-UX Linux Solaris  
./stopServer.sh server1
```

```
i5/OS Windows  
./stopServer server1
```

If a server is running and security is enabled, use the following command:

```
AIX HP-UX Linux Solaris  
./stopServer.sh server1 -user user_ID -password password
```

```
i5/OS Windows  
./stopServer server1 -user user_ID -password password
```

If you have multiple servers, you can use the serverStatus command to find running application servers associated with the target product instance. Issue the following command from the *profile_root/bin* directory to determine which servers, if any, are running:

```
AIX HP-UX Linux Solaris  
./serverStatus.sh -all
```

```
i5/OS Windows  
./serverStatus -all
```

6. Run the feature pack installation program using the `-silent` option.

Run the install executable file in the root directory of the feature pack installation image:

- **AIX** **HP-UX** **Linux** **Solaris** `./install -options responsefile.SCA.txt -silent`
- **Windows** `install -options responsefile.SCA.txt -silent`

The installation program runs silently in the background.

Results

The installation program records installation events in the installation log files and installs the feature pack.

After the program runs, examine the logs in *app_server_root/logs/sca/install* directory. If the feature pack does not install successfully, correct the problems identified in the logs and install the product again.

What to do next

If the product installs successfully, to use the feature pack functionality, create a new profile that is enabled for the Feature Pack for SCA using the Profile

Management tool or the `manageprofiles` command. Read the profile topics for more information.

Uninstalling the Feature Pack for SCA on distributed operating systems

Uninstall the feature pack product files, leaving the application server product intact.

Before you begin

The `uninstall` command calls the uninstaller program that is created during installation. The uninstaller program is customized for each product installation, with specific disk locations and routines for removing installed features.

Uninstall any feature packs first before you uninstall the application server. If you have a feature pack installed, uninstalling the WebSphere Application Server product using the uninstaller program might cause the feature-pack installation to fail. However, you should still uninstall the feature pack after uninstalling the application server to remove all feature-pack product entries and artifacts that might prevent a successful reinstallation. See [Troubleshooting](#) for more information.

Note: If a profile is augmented with the feature pack, then the feature pack uninstaller invokes unaugmentation actions for that profile before invoking the `uninstall` action.

Uninstallation unaugments application server profiles that were previously augmented for the feature pack, rendering them unusable.

1. Log on to the system.

AIX **HP-UX** **Linux** **Solaris** Log on using the same user ID that was used when the product was installed or as a user that has write permissions to the installation directory. Issue the `ls -al` command at the root of the WebSphere Application Server installation to find the user ID that was used to install the product.

Windows Log on as a user who belongs to the administrators group or as a user who has write permissions to the installation directory.

2. If the feature pack is installed on a Network Deployment product, perform the following tasks:
 - a. Stop the node agent process that might be running on the system.
For example, issue the following command from the `profile_root/bin` directory of a federated node on a Linux workstation to stop the node agent process:

```
./stopNode.sh
```


If servers are running and security is enabled, then use the following command:

```
./stopNode.sh -user user_ID -password password
```
 - b. Stop the deployment manager `dmgr` process.
For example, issue the following command on a Linux workstation from the `profile_root/bin` directory of the deployment manager profile:

```
./stopManager.sh -user user_ID -password password
```
3. Stop each running application server.

Stop all server processes in all profiles associated with the target product instance. For example, issue the following command from the *profile_root/bin* directory to stop the server1 process in the application server profile:

```
AIX HP-UX Linux Solaris  
./stopServer.sh server1
```

```
i5/OS Windows  
./stopServer server1
```

If a server is running and security is enabled, use the following command:

```
AIX HP-UX Linux Solaris  
./stopServer.sh server1 -user user_ID -password password
```

```
i5/OS Windows  
./stopServer server1 -user user_ID -password password
```

If you have multiple servers, you can use the serverStatus command to find running application servers associated with the target product instance. Issue the following command from the *profile_root/bin* directory to determine which servers, if any, are running:

```
AIX HP-UX Linux Solaris  
./serverStatus.sh -all
```

```
i5/OS Windows  
./serverStatus -all
```

- Optional: Back up configuration files, profiles, and log files to refer to them later if necessary.

Use the backupConfig command to back up configuration files and profiles. Read the "backupConfig command" topic for more information.

- Run the uninstall command in the *app_server_root/uninstall_sca* directory:
 - AIX** **HP-UX** **Linux** **Solaris** `uninstall.sh`
 - Windows** `uninstall.exe`

The uninstallation wizard begins and displays the Welcome panel.

You can also uninstall silently by running the uninstall command with the `silent` parameter:

```
uninstall -silent
```

- If you are using the wizard, then click **Next** to begin uninstalling the product. The uninstaller wizard displays a confirmation panel that lists a summary of the components that you are uninstalling.
 - Click **Next** to continue uninstalling the product.
 - Click **Finish** to close the wizard after the wizard removes the product.
- Review the uninstallation log files located in the *app_server_root/logs/uninstall/sca* directory.

Results

This procedure results in uninstalling the feature pack product. All profiles augmented with the feature pack were unaugmented during the feature pack uninstallation.

Troubleshooting

Linux Uninstalling the application server before uninstalling the feature pack might result in the failure of configuration actions that are responsible for

removing Linux shortcuts. Uninstall any feature pack installations first before uninstalling the application server to ensure that both products are uninstalled cleanly. If you have already uninstalled the application server, then run the feature pack uninstaller to clean up the feature pack installation and to remove any product registry entries. You can ignore the failed configuration actions from the application server uninstallation process. However, manually remove the entire application server directory afterwards.

Chapter 3. Installing the Feature Pack for SCA Version 1.0 on IBM i systems

The Feature Pack for Service Component Architecture (SCA) Version 1.0 is an optionally installable product extension for WebSphere Application Server that delivers an integrated, open implementation of SCA technology specified by IBM and other industry leaders through the Open SOA Collaboration.

Before you begin

Before starting this installation, complete the following actions:

1. Ensure that your user profile has *ALLOBJ and *SECADM special authorities.
2. Determine if the application server is already installed on your system. The feature pack must be installed on an existing application server installation.
 - a. Enter the Display Software Resources (DSPSWRSC) command on a CL command line.
 - b. Look for an entry with the product Resource ID 5733W70.
 - If you do not find the product Resource ID, then this product has not been installed on your server.
 - If you find the product Resources ID, ensure that at least one of the following entries is displayed:
 - 5733W70 2 5102 WebSphere Application Server V7.0
 - 5733W70 1 5101 WebSphere Application Server V7.0 Express
 - 5733W70 3 5103 WebSphere Application Server V7.0 Network Deployment
3. Install a WebSphere Application Server Version 7.0 product if you have not done so already.
4. Download the feature pack and extract the contents to an integrated file system (IFS) directory on the IBM i system on which you intend to install.

For example, create two directories, `sca_download` and `sca_installation_image`. Then, download the feature pack to the `sca_download` directory and then extract the downloaded file to the `sca_installation_image` directory. Do not move any files out of the `sca_installation_image` directory.
5. The operating system requirements for a feature pack are the same as the requirements for an application server installation. However, ensure that you have enough free disk space to install the feature pack onto the application server installation. The following space is required:
 - 1800 MB of free space available in your target installation directory. This estimate includes the application server maintenance bundled with the feature pack and is in addition to the existing application server product.
 - 600 MB of free space available in your temporary directory

Note: You must have the application server samples installed to use the SCA samples. If you did not install the application server samples, then remove any fixes or fix packs you have applied to the application server, run the application server installer and add the samples to your application server, and reinstall the fixes or fix packs.

Restriction: You cannot install a feature pack remotely. For example, you cannot install the product onto your IBM i system from a Windows workstation. You must install a feature pack on an IBM i system using a local command-line installation.

About this task

This topic describes how to install the Feature Pack for SCA silently using the installation program. You can install the feature pack from Qshell using the INSTALL command. You can also use the RUNJVA command to invoke the installation wizard.

1. Log on to the system with a user profile that has *ALLOBJ and *SECADM special authorities.
2. Copy the responsefile.SCA.txt file located in the root directory of the extracted installation image.
3. Edit the copy of the response file. You can edit the file using a mapped drive and a text editor or by using the EDTF CL command from the IBM i system command line.

Table 2. Feature-pack response-file options and descriptions.

Set values for the following options where *app_server_root* is the directory path to your WebSphere Application Server installation:

| Option | Description |
|--|--|
| -OPT silentInstallLicenseAcceptance="true" | You must accept the enclosed license agreement to install the feature pack. |
| -OPT installLocation= <i>app_server_root</i> | Set <i>app_server_root</i> to the root directory of your application server product. |
| -OPT disableNonBlockingPrereqChecking="true" | Uncomment this option in order to install application server fix packs, if they are required. The installer will fail if you have not uncommented this option and your application server still requires the fix packs bundled with the feature pack. Uncomment this line to notify the installer to continue with the installation and log the warnings even though prerequisite checking failed. |
| -OPT fepRefreshpackLocation=" <i>refresh_pack_location_and_file_name</i> " | Optional. The feature pack installer is capable of applying refresh packs and fix packs for the feature pack. However, applying higher level feature pack maintenance during installation is optional. Specify the directory paths and file names of the feature pack maintenance packages to apply during installation. Otherwise, leave these options commented out. |
| -OPT fepFixpackLocation=" <i>fix_pack_location_and_file_name</i> " | |

4. Stop all processes for the application server product on which you are installing the feature pack.

Stop the application server and any other product processes. For example, for the Network Deployment product, stop the deployment manager, the node agent, and all application server processes.

5. Verify that the host server jobs have started on your server.

The host server jobs allow the installation code to run on IBM i. On a CL command line, enter the following command:

```
STRHOSTSVR SERVER(*ALL)
```

6. Invoke the installation program for the feature pack.

Run the INSTALL command from Qshell or use the RUNJVA command from the CL command line.

In the following example commands, *path/responsefile* represents the fully qualified path of the response file that you edited:

- Run the INSTALL command from Qshell.
 - a. On a CL command line, issue the STRQSH command to start the Qshell command shell.

- b. Issue the installation command from the root directory of the extracted installation image to start the installation program:

```
install -options path/responsefile
```

Important: Do not exit the Qshell session (PF3) until the installation has completed. Doing so might cause the installation to stop prematurely.

- Or, issue the RUNJVA command from the CL command line:

At the CL command line, enter the RUNJVA command in the root directory of the extracted installation image. Enter the full command on one line. The command is shown here on multiple lines for formatting clarity:

```
RUNJVA
CLASS(run) PARM('-options' 'path/responsefile')
CLASSPATH('path/setup.jar')
PROP(
('Xbootclasspath/p' 'java/endorsed/xml.jar')
(java.version 1.5)
(is.debug 1)
)
```

7. For security purposes, if the host servers were not running prior to installation, run the end host server (ENDHOSTSVR) command after the installation is complete.

Results

The installation program records events in the log files located in the `app_server_root/logs/sca/install` directory.

What to do next

If the product installs successfully, to use the feature pack functionality, create a new profile using the Profile Management tool or the `manageprofiles` command.

Uninstalling the Feature Pack for SCA on IBM i systems

You can uninstall a feature pack product by running the feature pack uninstall command from your IBM i server.

Before you begin

The uninstall command calls the uninstaller program that is created during installation. The uninstaller program is customized for each product installation, with specific disk locations and routines for removing installed features.

Uninstall any feature packs first before you uninstall the application server. If you have a feature pack installed, then uninstalling the WebSphere Application Server product using the uninstaller program causes the feature pack to stop working. However, you should still uninstall the feature pack after uninstalling the application server to remove all feature pack product entries and artifacts which might prevent a successful reinstallation. See [Troubleshooting](#) for more information. This same limitation applies if you are uninstalling a *customized installation package* (CIP) created with IBM WebSphere Installation Factory.

Note: If a profile is augmented with the feature pack, then the feature pack uninstaller invokes unaugmentation actions for that profile before invoking the uninstall action.

About this task

Use this procedure to uninstall a feature pack from a WebSphere Application Server for IBM i installation.

1. Log on to the IBM i system with a user profile that has *ALLOBJ special authority.
2. Stop all processes for the application server product for which you are uninstalling the feature pack.

Stop the application server and any other product processes. For example, for the Network Deployment product, stop the deployment manager, the node agent, and all application server processes.

3. Verify that the host server jobs have started on your IBM i server.

The host server jobs allow the installation code to run on IBM i. On a CL command line, enter the following command:

```
STRHOSTSVR SERVER(*ALL)
```

4. Uninstall the feature pack from your WebSphere Application Server on your IBM i server.

To uninstall the feature pack, run the following command from the Qshell command line in the *app_server_root/uninstall_sca* directory:

```
uninstall -silent
```

Results

After completing the procedure, the feature pack is uninstalled. Uninstalling the feature pack from the IBM i server removes feature pack libraries and directories, and unaugments any profiles which were augmented with the feature pack.

If the feature pack does not uninstall successfully, examine the logs in the *app_server_root/logs/sca/uninstall* directory to identify why the uninstallation failed. Correct the problems identified and try uninstalling the product again.

Chapter 4. Installing the Feature Pack for SCA Version 1.0 on z/OS systems

You can use the System Modification Program / Extended (SMP/E) to install the Feature Pack for SCA Version 1.0 on WebSphere Application Server for z/OS Version 7.0 .

Before you begin

The Feature Pack for Service Component Architecture (SCA) is an optionally installable product extension for WebSphere Application Server that delivers an integrated, open implementation of SCA technology specified by IBM and other industry leaders through the Open SOA Collaboration. Quality-of-service capabilities such as transactions and security, and ease-of-use features, such as policy-set definitions for Web Services are available with the feature pack. This integration ensures that all of WebSphere's capabilities work together with SCA applications to provide a natural environment for both the SCA and existing applications.

Before starting this installation, perform the following actions:

- Install the WebSphere Application Server for z/OS Version 7.0 product code and optional materials if you have not done so already.
- Install the WebSphere Customization Tools, which contain the Profile Management Tool, if you are going to use it to create the jobs for enabling profiles for the feature pack.

The latest version of the WebSphere Customization Tools can be downloaded from IBM WebSphere Customization Tools.

About this task

The Feature Pack for SCA is included as service with the WebSphere Application Server for z/OS optional materials.

1. Obtain the program temporary fix (PTF) numbers for the Feature Pack for SCA product code from the WebSphere Application Server for z/OS service support Web site.
2. Order or download the appropriate PTFs.
3. Verify that you are running the minimum level of WebSphere Application Server for z/OS that is required by the feature pack, and install any WebSphere Application Server for z/OS maintenance that is needed.
4. Install the product PTFs for the Feature Pack for SCA.

Follow the instructions provided in the PTFs. The product files for the feature pack are installed into the following directory:

```
-PathPrefix-/usr/lpp/zWebSphere_0M/V7R0/FPSCA
```

The file system containing this directory must be mounted on all z/OS systems on which the feature pack will be used.

What to do next

- Install the Feature Pack for SCA extension for the Profile Management Tool.
 1. Make sure that you have installed WebSphere Customization Tools Version 7.0.0.7 or later on your workstation.

You can download the latest version of WebSphere Customization Tools from the following Web sites:

- WebSphere Customization Tools for Windows
 - WebSphere Customization Tools for Linux
2. Make sure that you performed the SMP/E installation of the WebSphere Application Server Version 7.0 Feature Pack for SCA on your z/OS system.
 3. Create a folder on your workstation to receive the file to be downloaded from the z/OS system.
 4. Using FTP, download the following file in binary format from the z/OS system where the WebSphere Application Server for z/OS Optional Materials program is installed. For example:

```
/usr/lpp/zWebSphere_0M/V7R0/FPSCA/util/WCT/sca.wct
```
 5. Open the WebSphere Customization Tools on your workstation, and go to **Help > Software Updates > Install Extension**.
 6. On the Extension Locations panel, click **Install new extension location**.
 7. On the Source Archive File panel, use the **Browse** button to specify the path to the sca.wct file that you downloaded from the SMP/E location and then click **Next**.
 8. On the Summary Location panel, click **Next**.
 9. On the Install Successful panel, perform the following actions:
 - a. Select the entire contents of the Location field and copy them to the clipboard.
 - b. To be certain that you captured the location, paste it into a text-editor session.
 - c. Click **Finish**.
 10. In the Product Configuration panel that displays, click **Add an Extension Location**.

Notes:

- You can always access this panel directly by going to **Help > Software Updates > Product Configuration**.
 - Do not use any other feature or link on this panel other than **Add an Extension Location**. The other tasks listed on this panel are not supported in the WebSphere Customization Tools environment.
11. In the panel that displays, paste the copied location into the Folder field and click **OK**.
 12. Click **Yes** on the panel asking you if you would like to restart the WebSphere Customization Tools.

Note: You might need to manually restart the WebSphere Customization Tools if it does not restart automatically.

13. Verify the proper installation of the extension.
 - a. Go to **Help > About WebSphere Customization Tools**.
 - b. Click **Feature Details**.
 - c. Make sure that the Feature Pack for SCA appears in the list.

When you have finished the installation, you can create a WebSphere Application Server on z/OS runtime environment that includes Feature Pack for SCA functions.

To use the feature-pack functionality, you must create a new profile with the feature-pack functionality or augment an existing profile with the feature pack.

Use the workstation-based Profile Management Tool, which can be launched from the WebSphere Customization Tools, or the `zpmt` command to generate customization jobs and associated instructions for Feature Pack for SCA profile creation and augmentation.

Important: Back up your configuration file system before augmenting any profiles. You cannot unaugment profiles, and you might want to restore your pre-augmentation configuration later. After you restore, you will have to manually make any other changes that you made to the configuration after the backup.

Augmentation rules and limitations for feature packs on z/OS

Profile augmentation depends on the type of profile, whether you changed the configuration information, and so on. You must have the correct combination of feature packs in order to add a node, manage clusters, install applications, and manage server templates. Use these rules and limitations to ensure a properly functioning feature-pack environment.

You can have a mix of augmented and unaugmented profiles that share a single WebSphere Application Server installation. Feature-pack functionality is available only within profiles that have been augmented.

Augmentation rules and limitations

- The latest feature pack that you apply might require augmentation of the Network Deployment profiles or the profile of a prerequisite feature pack. If so, you can have a mix of augmented and unaugmented profiles. However, you must have at least one profile augmented with this latest feature pack to use its capabilities.
- For multiple feature packs, you must first install all the feature packs, augment the profile with each of the feature packs, and then make configuration changes for those feature packs. The order of installing or augmenting the feature packs does not matter, unless a particular feature pack requires you to install another feature pack first. You can only make configuration changes after you augment the profile.
- Back up your configuration file system before augmenting profiles.

Table 3. Rules for profile augmentation.

The following table provides additional augmentation rules for particular types of profiles with this feature pack.

| Profile | Supported | Not supported |
|-------------------------------|---|---------------|
| Standalone application server | <ul style="list-style-type: none"> • Creation of a new standalone application server that is enabled for the Feature Pack for SCA <p>When you create the standalone application server profile for the feature pack, the feature pack automatically augments the profile with Feature Pack for SCA capabilities.</p> <ul style="list-style-type: none"> • Augmentation of an existing Version 8.0 standalone application server profile with the Feature Pack for SCA | |

Table 3. Rules for profile augmentation (continued).

The following table provides additional augmentation rules for particular types of profiles with this feature pack.

| Profile | Supported | Not supported |
|-------------------------|---|---|
| Deployment manager | <ul style="list-style-type: none"> Creation of a new deployment manager that is enabled for the Feature Pack for SCA When you create the deployment manager profile for the feature pack, the feature pack automatically augments the profile with Feature Pack for SCA capabilities. Augmentation of an existing deployment manager profile with the Feature Pack for SCA This action is supported as long as all of the federated nodes in the cell are Version 8.0 or higher. You might have made configuration changes to the deployment manager profile. | Augmentation of an existing deployment manager profile if the version of any federated node in the cell is lower than Version 7.0 |
| Managed (custom) node | <ul style="list-style-type: none"> Creation of a new managed (custom) node that is enabled for the Feature Pack for SCA When you create the managed (custom) node for the feature pack, the feature pack automatically augments the profile with Feature Pack for SCA capabilities. Augmentation of an existing managed (custom) node with the Feature Pack for SCA | |
| Network Deployment cell | <ul style="list-style-type: none"> Creation of a new Network Deployment cell profile that is enabled for the Feature Pack for SCA When you create the deployment manager and the federated application server for the cell, the feature pack automatically augments the profile with Feature Pack for SCA capabilities. Augmentation of an existing Network Deployment cell with the Feature Pack for SCA You must enable a deployment manager and application server for the feature pack based on the preceding rules in this table. | |
| Administrative agent | | <p>Creation or augmentation of an administrative agent to enable it for a feature pack</p> <p>However, you can use an administrative agent in a feature-pack environment.</p> |
| Job manager | | <p>Creation or augmentation of a job manager to enable it for a feature pack</p> <p>However, you can use a job manager in a feature-pack environment.</p> |
| Secure proxy server | | <p>Creation or augmentation of a secure proxy server to enable it for a feature pack</p> <p>However, you can use a secure proxy server in a feature-pack environment.</p> |

Table 3. Rules for profile augmentation (continued).

The following table provides additional augmentation rules for particular types of profiles with this feature pack.

| Profile | Supported | Not supported |
|-----------------------------------|-----------|---|
| Secure proxy administrative agent | | <p>Creation or augmentation of a secure proxy administrative agent to enable it for a feature pack</p> <p>However, you can use a secure proxy administrative agent in a feature-pack environment.</p> |

Augmentation rules and limitations in a mixed-cell environment

Table 4. Augmentation in a mixed-cell environment.

When you perform tasks between nodes or between nodes and the deployment manager, the feature packs must be compatible.

| Function | Rules |
|-----------------------------------|--|
| Addition of a node | <ul style="list-style-type: none"> You can add a node to a cell as long as the deployment manager has been augmented with at least the same set of feature packs as the node. The deployment manager might have been augmented with additional feature packs. You can add a node with no feature-pack profile to a cell even though the deployment manager is augmented with some feature packs; however, the node that you add must be at Version 8.0 or higher. You cannot add a node with a particular feature-pack profile to a cell if the deployment manager has not been augmented with that feature pack. |
| Application installation | <ul style="list-style-type: none"> You can target an application that requires feature-pack functionality to an application server on a node that has been augmented with feature packs that contain that functionality. You cannot target an application that requires feature-pack functionality to an application server on a node that has not been augmented with that feature-pack functionality. You can target an application that does not require feature-pack functionality to an application server on a node with or without feature-pack augmentation. |
| Server configuration template use | <ul style="list-style-type: none"> You can use the server configuration template to create a server on another node that is augmented with the same feature pack. If you attempt to use a server configuration template to create a server on another node that is augmented with a different feature pack, the operation fails. The scenario is not supported. |
| Cluster management | <ul style="list-style-type: none"> When you add a new member to a cluster, the new member must be able to run all the applications that have been targeted for the cluster. If an application targeted for the cluster requires a specific feature pack, you must add the new member from a node that is enabled with that feature pack; otherwise, an error occurs. If no application on the cluster requires a specific feature pack, you can add the new member to the cluster from a node with or without a feature pack. |

Table 4. Augmentation in a mixed-cell environment (continued).

When you perform tasks between nodes or between nodes and the deployment manager, the feature packs must be compatible.

| Function | Rules |
|---|---|
| Configuration-archive export and import | <ul style="list-style-type: none"> If a configuration contains feature-pack capabilities, exporting a configuration to a configuration archive and importing a configuration from a configuration archive are not supported. If you run one of the import or export commands of the ConfigArchiveOperations command group against one of these configurations, the command might complete without reporting an error. No message is displayed when importing or exporting; however, no confirmation exists for imported configuration success. |

Important: Back up your configuration file system before augmenting any profiles. You cannot unaugment profiles, and you might want to restore your pre-augmentation configuration later. After you restore, you will have to manually make any other changes that you made to the configuration after the backup.

Unaugmentation rule

You cannot unaugment profiles that have been enabled with feature-pack functionality in WebSphere Application Server for z/OS Version 7.0.

Configuring with the Profile Management Tool

Use the z/OS Profile Management Tool on a workstation running the Windows or Linux Intel® operating system to generate the customization definitions for creating new profiles with the feature pack installed and enabling existing profiles for the feature pack, and then use the tool to upload the associated jobs and instructions to the target z/OS system.

About this task

WebSphere Application Server for z/OS application serving environment nodes are created using batch jobs that are built with the Profile Management Tool or the zpmt command. After the node is configured and running, make further changes using the administrative console or scripting tool.

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, “Installing the Feature Pack for SCA Version 1.0 on z/OS systems,” on page 17.
2. Install the workstation-based WebSphere Customization Tools Version 7.0.0.7 or later, which includes the Profile Management Tool.
You can download the latest version of WebSphere Customization Tools from the following Web sites:
 - WebSphere Customization Tools for Windows
 - WebSphere Customization Tools for Linux
3. Install the feature-pack extension for the Profile Management Tool.
4. Check that an FTP server is running on the z/OS target system.
5. Choose the task for the type of environment that you want to configure from the following tasks:

- “Using the Profile Management Tool to create z/OS standalone application servers with the Feature Pack for SCA installed”
- “Using the Profile Management Tool to enable existing z/OS standalone application servers for the Feature Pack for SCA” on page 33
- “Using the Profile Management Tool to create z/OS deployment managers with the Feature Pack for SCA installed” on page 36
- “Using the Profile Management Tool to enable existing z/OS deployment managers for the Feature Pack for SCA” on page 46
- “Using the Profile Management Tool to create z/OS managed (custom) nodes with the Feature Pack for SCA installed” on page 49
- “Using the Profile Management Tool to enable existing z/OS managed (custom) nodes for the Feature Pack for SCA” on page 58
- “Using the Profile Management Tool to create z/OS Network Deployment cells with the Feature Pack for SCA installed” on page 61

Using the Profile Management Tool to create z/OS standalone application servers with the Feature Pack for SCA installed

You can use the Profile Management Tool to generate the jobs required to create a z/OS application server with the Feature Pack for SCA installed.

Before you begin

Before starting this procedure, perform the following actions:

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, “Installing the Feature Pack for SCA Version 1.0 on z/OS systems,” on page 17.
 2. Install the workstation-based WebSphere Customization Tools, which include the Profile Management Tool.
 3. Install the Feature Pack for SCA extension for the Profile Management Tool.
 4. Plan your application server environment, and fill out a copy of the “z/OS customization worksheet: Standalone application servers with the Feature Pack for SCA” on page 25.
1. Start the Profile Management Tool.
 2. Optional: If you want to add a customization location to the **Customization Locations** table, perform the following actions:
 - a. Click **Add**.
 - b. Enter the path name of the location where you want to store the customization definitions and associated data.

Important: The customization location directory must be empty when you create a new customization location.
 - c. Perform one of the following actions:
 - If you want to use an existing customization location, select **Use an existing customization location**.
 - If you want to create a new customization location, select **Create a new customization location**.
Enter a value for the name that is meaningful to you, and select Version 7.0.
 - d. Click **Finish**.
 3. Create a customization definition that includes the Feature Pack for SCA.

For more information, read “z/OS customization worksheet: Standalone application servers with the Feature Pack for SCA” on page 25.

- a. In the **Customization Locations** table, select the location of the customization definition that you want to create.
- b. Click the **Customization Definitions** tab if it is not already selected.
- c. Click **Create**.
- d. Expand **WebSphere Application Server Feature Pack for SCA Version 1.0**.
- e. Select **Application server with Feature Pack for SCA Version 1.0**.
- f. Click **Next**.
- g. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

- h. Click **Create**.
- i. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
 - If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.
4. Review the standalone application server definition response file to confirm that the values are correct.
 5. Upload the customization jobs and instructions to the target z/OS system.
 6. Follow the generated instructions, which you can view using one of the following methods:
 - In the Profile Management Tool, select the desired customization definition and select the **Customization Instructions** tab.
 - After you upload the definition, view member BBOSSINS in the target CNTL dataset, which will be identified on the upload panel.
 7. If you encounter problems caused by your values in the customization definition, modify your variables using the Profile Management Tool, regenerate the instructions, and upload the customization definitions again.

Notes:

- Do not attempt to fix a typographical error or make a change by modifying the generated output. Many of the variables are used in multiple members of the target datasets; if you do not change them all, therefore, you might experience errors that are difficult to diagnose.

- Remember that you cannot upload new customization jobs while either configuration dataset is open.

Results

You have set up a new z/OS standalone application server with the Feature Pack for SCA installed.

z/OS customization worksheet: Standalone application servers with the Feature Pack for SCA

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this standalone application server:

System name: _____

Sysplex name: _____

Table 5. Customization Definition Name.

Enter your values:

| Item | Default | Your value |
|------------------------------------|--------------|------------|
| Customization definition name | ZSCAAppSrvxx | |
| Response file path name (optional) | None | |

Table 6. Default Values.

Enter your values:

| Item | Default | Your value |
|---|--------------|------------|
| GID and UID defaults | | |
| Set each default GID and UID value to indicate OS security is to assign an unused value | Not selected | |
| Name and userid defaults | | |
| Application server will be federated into a Network Deployment cell | Not selected | |
| Set default names and userids based on cell, system, and cluster identifiers | Not selected | |
| Two-character cell identifier | AZ | |
| Two-character cluster identifier | 00 | |
| Single-character system identifier | A | |
| Port defaults | | |

Table 6. Default Values (continued).

Enter your values:

| Item | | Default | Your value |
|------|---|--------------|------------|
| | Set default port values from the following port range | Not selected | |
| | Lowest default port number | 9530 | |
| | Highest default port number | 9549 | |

Table 7. Target Datasets.

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| High-level qualifier (HLQ) | None | |

Table 8. Configure Common Groups.

Enter your values:

| Item | | Default | Your value |
|--|---------------------------------|--------------|------------|
| WebSphere Application Server configuration group information | | | |
| | Group | WSCFG1 | |
| | Allow OS security to assign GID | Not selected | |
| | Assign user-specified GID | Selected | |
| | Specified GID | 2500 | |
| WebSphere Application Server servant group information | | | |
| | Group | WSSR1 | |
| | Allow OS security to assign GID | Not selected | |
| | Assign user-specified GID | Selected | |
| | Specified GID | 2501 | |
| WebSphere Application Server local user group information | | | |
| | Group | WSCLGP | |
| | Allow OS security to assign GID | Not selected | |
| | Assign user-specified GID | Selected | |
| | Specified GID | 2502 | |

Table 9. Configure Common Users.

Enter your values:

| Item | Default | Your value |
|---------------------------|---------|------------|
| Common controller user ID | | |

Table 9. Configure Common Users (continued).

Enter your values:

| Item | | Default | Your value |
|---|---------|---------------------------------|--------------|
| | User ID | WSCRU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2431 |
| Common servant user ID | | | |
| | User ID | WSSRU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2432 |
| WebSphere Application Server administrator | | | |
| | User ID | WSADMIN | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2403 |
| Asynchronous administration user ID | | | |
| | User ID | WSADMSH | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2504 |
| WebSphere Application Server user ID home directory | | /var/ WebSphere/ home | |

Table 10. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.1 or later, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

| Item | | Default | Your value |
|----------------------------|---------|---------------------------------|--------------|
| Controller adjunct user ID | | | |
| | User ID | WSCRAU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2433 |
| Daemon user ID | | | |
| | User ID | WSDMNU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2434 |

Table 11. System and Dataset Names.

Enter your values:

| Item | Default | Your value |
|----------------------|--------------|------------|
| System name | None | |
| Sysplex name | None | |
| PROCLIB dataset name | SYS1.PROCLIB | |

Table 12. Cell, Node, and Server Names.

Enter your values:

| Item | Default | Your value |
|-------------------------|------------|--------------|
| Cell names | | |
| | Short name | BBOBASE |
| | Long name | bbobase |
| Node names | | |
| | Short name | BBONODE |
| | Long name | bbonode |
| Server names | | |
| | Short name | BBOS001 |
| | Long name | server1 |
| Cluster transition name | BBOC001 | |
| JVM mode | | |
| | 31 bit | Not selected |
| | 64 bit | Selected |

Table 13. Configuration File System.

Enter your values:

| Item | Default | Your value |
|---|--|--------------|
| Mount point | /wasv7config/ cell_long_name/ node_long_name | |
| Directory path name relative to mount point | AppServer | |
| Dataset name | OMVS.WAS70. cell_short_name. node_short_name.HFS | |
| File system type | | |
| | Hierarchical File System (HFS) | Selected |
| | zSeries® File System (ZFS) | Not selected |
| Volume, or '*' for SMS | * | |
| Primary allocation in cylinders | 450 | |
| Secondary allocation in cylinders | 100 | |

Table 14. WebSphere Application Server Product File System.

Enter your values:

| Item | | Default | Your value |
|-------------------------------|---|--|------------|
| Product file system directory | | /usr/lpp/ zWebSphere/ V7R0 | |
| Intermediate symbolic link | | | |
| | Create intermediate symbolic link | Selected | |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ node_long_name/ wassmpe | |

Table 15. Feature Pack for SCA Product File System.

Enter your values:

| Item | | Default | Your value |
|-------------------------------|---|--|------------|
| Product file system directory | | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | | |
| | Create intermediate symbolic link | Selected | |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ node_long_name/ fpscasmpe | |

Table 16. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.5 or later, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

| Item | | Default | Your value |
|----------------------|--|-------------------|------------|
| Error log stream | | | |
| | Error log stream name (optional) | BBOBASE.ERROR.LOG | |
| CTRACE parmli member | | | |
| | CTRACE parmli member suffix (optional) | 60 | |

Table 17. Optional Application Deployment.

Enter your values:

| Item | Default | Your value |
|-----------------------------------|--------------|------------|
| Deploy the administrative console | Selected | |
| Deploy the default application | Selected | |
| Deploy the sample applications | Not selected | |

Table 18. Process Definitions.

Enter your values:

| Item | Default | Your value |
|--|---------------------------|---------------------------|
| Controller process | | |
| Job name | <i>server_short_name</i> | <i>server_short_name</i> |
| Procedure name | BBO7ACR | |
| Controller adjunct process | | |
| Job name | <i>server_short_nameA</i> | <i>server_short_nameA</i> |
| Procedure name | BBO7CRA | |
| Servant process | | |
| Job name | <i>server_short_nameS</i> | <i>server_short_nameS</i> |
| Procedure name | BBO7ASR | |
| Admin asynch operations procedure name | BBO7ADM | |

Table 19. Port Values Assignment.

Enter your values:

| Item | Default | Your value |
|--|---------|------------|
| Node host name or IP address | None | |
| JMX SOAP connector port | 8880 | |
| ORB listener IP address | * | |
| ORB port | 2809 | |
| ORB SSL port | 0 | |
| HTTP transport IP address | * | |
| Administrative console port | 9060 | |
| Administrative console secure port | 9043 | |
| HTTP transport port | 9080 | |
| HTTPS transport port | 9443 | |
| Administrative interprocess communication port (K) | 9633 | |

Table 19. Port Values Assignment (continued).

Enter your values:

| Item | Default | Your value |
|---|---------|------------|
| High Availability Manager communication port (DCS) | 9353 | |
| Service integration port | 7276 | |
| Service integration secure port | 7286 | |
| Service integration MQ interoperability port | 5558 | |
| Service integration MQ interoperability secure port | 5578 | |
| Session initiation protocol (SIP) port | 5060 | |
| Session initiation protocol (SIP) secure port | 5061 | |

Table 20. Location Service Daemon Definitions.

Enter your values:

| Item | Default | Your value |
|------------------------------|---|---|
| Daemon home directory | /wasv7config/ cell_long_name/ node_long_name/Daemon | /wasv7config/cell_long_name/ node_long_name/Daemon |
| Daemon job name | BBODMNB | |
| Procedure name | BBO7DMNB | |
| IP name | host_name | |
| Listen IP | * | |
| Port | 5655 | |
| SSL port | 5656 | |
| Register daemon with WLM DNS | Not selected | |

Table 21. SSL Customization.

Enter your values:

| Item | Default | Your value |
|---|----------------------------|------------|
| Certificate authority keylabel | WebSphereCA | |
| Generate certificate authority (CA) certificate | Selected | |
| Expiration date for certificates | 2018/12/31 | |
| Default SAF keyring name | WASKeyring.cell_short_name | |
| Enable SSL on location service daemon | Selected | |

Table 22. Administrative Security Selection.

Enter your values:

| Item | Default | Your value |
|----------------------------------|--------------|------------|
| Use a z/OS security product | Selected | |
| Use WebSphere Application Server | Not selected | |
| Do not enable security | Not selected | |

Table 23. Security Managed by the z/OS Product.

Enter your values:

| Item | Default | Your value |
|---|------------------------|------------|
| SAF profile prefix | <i>cell_short_name</i> | |
| WebSphere Application Server unauthenticated user | | |
| User ID | WSGUEST | |
| Allow OS security to assign UID | Not selected | |
| Assign user-specified UID | Selected | |
| UID | 2402 | |
| Enable writable SAF keyring support | Not selected | |

Table 24. Security Managed by the WebSphere Family Product.

Enter your values:

| Item | Default | Your value |
|---------------------|---------|------------|
| User name | WSADMIN | |
| Password | None | |
| Sample applications | | |
| User name | samples | samples |
| Password | None | |

Table 25. Security Certificate.

Enter your values:

| Item | Default | Your value |
|------------------------------|--|------------|
| Default personal certificate | | |
| Issued to distinguished name | <i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i> | |
| Issued by distinguished name | <i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i> | |
| Expiration period in years | 1 | |

Table 25. Security Certificate (continued).

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| Root signing certificate | | |
| Expiration period in years | 20 | |
| Default keystore password | | |

Table 26. Web Server Definition (Part 1).

Enter your values:

| Item | Default | Your value |
|------------------------------------|------------------|--------------|
| Create a Web server definition | | Not selected |
| Web server type | IBM HTTP Server | |
| Web server operating system | z/OS | |
| Web server name | webserver1 | |
| Web server host name or IP address | <i>host_name</i> | |
| Web server port | 80 | |

Table 27. Web Server Definition (Part 2).

Enter your values:

| Item | Default | Your value |
|--|--------------------------|------------|
| Web server installation directory path | /etc/websrv1 | |
| Web server plug-in installation directory path | /etc/websrv1/ Plugins | |

Table 28. Job Statement Definition.

Enter your values:

| Item | Default | Your value |
|---------------|--|------------|
| //jobname JOB | (ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM | |
| //* | //* | |
| //* | //* | |
| //* | //* | |

Using the Profile Management Tool to enable existing z/OS standalone application servers for the Feature Pack for SCA

You can use the Profile Management Tool to enable the Feature Pack for SCA on an existing z/OS standalone application server.

Before you begin

Before starting this procedure, perform the following actions:

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, “Installing the Feature Pack for SCA Version 1.0 on z/OS systems,” on page 17.
2. Install the workstation-based WebSphere Customization Tools, which include the Profile Management Tool.
3. Install the Feature Pack for SCA extension for the Profile Management Tool.
4. Select the application server that you want to enable for the feature pack, and fill out a copy of the “z/OS augmentation worksheet: Standalone application servers with the Feature Pack for SCA” on page 35.

1. Start the Profile Management Tool.
2. Create a customization definition for augmenting a profile with the Feature Pack for SCA.

For more information, read “z/OS augmentation worksheet: Standalone application servers with the Feature Pack for SCA” on page 35.

- a. In the **Customization Locations** table, select the location of the customization definition that you want to create.
- b. Click the **Customization Definitions** tab if it is not already selected.
- c. Click **Augment**.
- d. Select **Application server**.
- e. Click **Next**.
- f. Select **Application server with Feature Pack for SCA Version 1.0**.
- g. Click **Next**.
- h. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

- i. Click **Augment**.
- j. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
 - If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.
3. Review the customization definition response file to confirm that the values are correct.
 4. Upload the customization jobs and instructions to the target z/OS system.

5. Follow the generated instructions, which you can view using one of the following methods:
 - In the Profile Management Tool, select the desired customization definition and select the **Customization Instructions** tab.
 - After you upload the definition, view the IWODINSA job in the target CNTL dataset, which contains a text version of the instructions.
6. If you encounter problems caused by your values in the customization definition, modify your variables using the Profile Management Tool, regenerate the instructions, and upload the customization definitions again.

Notes:

- Do not attempt to fix a typographical error or make a change by modifying the generated output. Many of the variables are used in multiple members of the target datasets; if you do not change them all, therefore, you might experience errors that are difficult to diagnose.
- Remember that you cannot upload new customization jobs while either configuration dataset is open.

Results

Your existing WebSphere Application Server for z/OS standalone application server is now enabled for the Feature Pack for SCA.

z/OS augmentation worksheet: Standalone application servers with the Feature Pack for SCA

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this standalone application server:

System name: _____

Sysplex name: _____

Table 29. Customization Definition Name.

Enter your values:

| Item | Default | Your value |
|------------------------------------|-----------------|------------|
| Customization definition name | ZSCAAugAppSrvxx | |
| Response file path name (optional) | None | |

Table 30. Target Datasets.

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| High-level qualifier (HLQ) | None | |

Table 31. Base File Systems.

Enter your values:

| Item | Default | Your value |
|--|-------------------------------|------------|
| Configuration file system | | |
| Mount point | /wasv7config | |
| Directory path name relative to mount point | AppServer | |
| WebSphere Application Server product file system | | |
| Product file system directory (or path name of intermediate symbolic link) | /usr/lpp/ zWebSphere/ V7R0 | |

Table 32. Feature Pack for SCA Product File System.

Enter your values:

| Item | Default | Your value |
|-------------------------------|--|----------------------------|
| Product file system directory | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | |
| | Create intermediate symbolic link | Selected |
| | Path name of intermediate symbolic link | /wasv7config/ fpscasmpe |

Table 33. Target Node Administrative Security.

Enter your values:

| Item | Default | Your value |
|---|-------------------------------|------------|
| Target node is managed by a z/OS security product | Selected | |
| | SAF profile prefix (optional) | None |

Table 34. Job Statement Definition.

Enter your values:

| Item | Default | Your value |
|---------------|--|------------|
| //jobname JOB | (ACCTNO,ROOM), 'USERID', CLASS=A, REGION=OM | |
| //* | //* | |
| //* | //* | |
| //* | //* | |

Using the Profile Management Tool to create z/OS deployment managers with the Feature Pack for SCA installed

You can use the Profile Management Tool to generate the jobs required to create a z/OS deployment manager with the Feature Pack for SCA installed.

Before you begin

Before starting this procedure, perform the following actions:

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, “Installing the Feature Pack for SCA Version 1.0 on z/OS systems,” on page 17.
2. Install the workstation-based WebSphere Customization Tools, which include the Profile Management Tool.
3. Install the Feature Pack for SCA extension for the Profile Management Tool.
4. Plan your Network Deployment environment, and fill out a copy of the “z/OS customization worksheet: Deployment managers with the Feature Pack for SCA” on page 38.

1. Start the Profile Management Tool.
2. Optional: If you want to add a customization location to the **Customization Locations** table, perform the following actions:
 - a. Click **Add**.
 - b. Enter the path name of the location where you want to store the customization definitions and associated data.

Important: The customization location directory must be empty when you create a new customization location.

- c. Perform one of the following actions:
 - If you want to use an existing customization location, select **Use an existing customization location**.
 - If you want to create a new customization location, select **Create a new customization location**.
Enter a value for the name that is meaningful to you, and select Version 7.0.
 - d. Click **Finish**.
3. Create a customization definition that includes the Feature Pack for SCA.
For more information, read “z/OS customization worksheet: Deployment managers with the Feature Pack for SCA” on page 38.
 - a. In the **Customization Locations** table, select the location of the customization definition that you want to create.
 - b. Click the **Customization Definitions** tab if it is not already selected.
 - c. Click **Create**.
 - d. Expand **WebSphere Application Server Feature Pack for SCA Version 1.0**.
 - e. Select **Management with Feature Pack for SCA Version 1.0**.
 - f. Click **Next**.
 - g. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

- h. Click **Create**.
- i. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
 - If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.
4. Review the deployment manager definition response file to confirm that the values are correct.
 5. Upload the customization jobs and instructions to the target z/OS system.
 6. Follow the generated instructions, which you can view using one of the following methods:
 - In the Profile Management Tool, select the desired customization definition and select the **Customization Instructions** tab.
 - After you upload the definition, view member BBOCCINS in the target CNTL dataset, which will be identified on the upload panel.
 7. If you encounter problems caused by your values in the customization definition, modify your variables using the Profile Management Tool, regenerate the instructions, and upload the customization definitions again.

Notes:

- Do not attempt to fix a typographical error or make a change by modifying the generated output. Many of the variables are used in multiple members of the target datasets; if you do not change them all, therefore, you might experience errors that are difficult to diagnose.
- Remember that you cannot upload new customization jobs while either configuration dataset is open.

Results

You have set up a new z/OS deployment manager with the Feature Pack for SCA installed.

z/OS customization worksheet: Deployment managers with the Feature Pack for SCA

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this deployment manager:

System name: _____

Sysplex name: _____

Table 35. Customization Definition Name.

Enter your values:

| Item | Default | Your value |
|------------------------------------|------------|------------|
| Customization definition name | ZSCADMgrxx | |
| Response file path name (optional) | None | |

Table 36. Default Values.

Enter your values:

| Item | Default | Your value |
|--------------------------|---|--------------|
| GID and UID defaults | | |
| | Set each default GID and UID value to indicate OS security is to assign an unused value | Not selected |
| Name and userid defaults | | |
| | Set default names and userids based on a cell identifier | Not selected |
| | Two-character cell identifier | AZ |
| Port defaults | | |
| | Set default port values from the following port range | Not selected |
| | Lowest default port number | 9510 |
| | Highest default port number | 9529 |

Table 37. Target Datasets.

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| High-level qualifier (HLQ) | None | |

Table 38. Configure Common Groups.

Enter your values:

| Item | Default | Your value |
|--|---------------------------------|--------------|
| WebSphere Application Server configuration group information | | |
| | Group | WSCFG1 |
| | Allow OS security to assign GID | Not selected |
| | Assign user-specified GID | Selected |
| | Specified GID | 2500 |
| WebSphere Application Server servant group information | | |

Table 38. Configure Common Groups (continued).

Enter your values:

| Item | | Default | Your value |
|---|-------|---------------------------------|--------------|
| | Group | WSSR1 | |
| | | Allow OS security to assign GID | Not selected |
| | | Assign user-specified GID | Selected |
| | | Specified GID | 2501 |
| WebSphere Application Server local user group information | | | |
| | Group | WSCLGP | |
| | | Allow OS security to assign GID | Not selected |
| | | Assign user-specified GID | Selected |
| | | Specified GID | 2502 |

Table 39. Configure Common Users.

Enter your values:

| Item | | Default | Your value |
|---|---------|---------------------------------|--------------|
| Common controller user ID | | | |
| | User ID | WSCRU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2431 |
| Common servant user ID | | | |
| | User ID | WSSRU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2432 |
| WebSphere Application Server administrator | | | |
| | User ID | WSADMIN | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2403 |
| WebSphere Application Server user ID home directory | | /var/ WebSphere/ home | |

Table 40. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.1 or later, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

| Item | Default | Your value |
|----------------|---------|------------|
| Daemon user ID | | |

Table 40. Configure Additional Users (continued).

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.1 or later, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

| Item | | Default | Your value |
|------|---------------------------------|--------------|------------|
| | User ID | WSDMNU1 | |
| | Allow OS security to assign UID | Not selected | |
| | Assign user-specified UID | Selected | |
| | Specified UID | 2434 | |

Table 41. System and Dataset Names.

Enter your values:

| Item | Default | Your value |
|----------------------|--------------|------------|
| System name | None | |
| Sysplex name | None | |
| PROCLIB dataset name | SYS1.PROCLIB | |

Table 42. Cell, Node, and Server Names.

Enter your values:

| Item | | Default | Your value |
|-------------------------|------------|---------|------------|
| Cell names | | | |
| | Short name | BBOCELL | |
| | Long name | bbocell | |
| Node names | | | |
| | Short name | BBODMGR | |
| | Long name | bbodmgr | |
| Server names | | | |
| | Short name | BBODMGR | |
| | Long name | dmgr | dmgr |
| Cluster transition name | | BBODMGR | |

Table 43. Configuration File System.

Enter your values:

| Item | Default | Your value |
|---|--|------------|
| Mount point | /wasv7config/ cell_long_name/ node_long_name | |
| Directory path name relative to mount point | DeploymentManager | |
| Dataset name | OMVS.WAS70. cell_short_name. node_short_name.HFS * | |

Table 43. Configuration File System (continued).

Enter your values:

| Item | | Default | Your value |
|---|--------------------------------|--------------|------------|
| File system type | | | |
| | Hierarchical File System (HFS) | Selected | |
| | zSeries File System (ZFS) | Not selected | |
| Volume, or '*' for SMS | | * | |
| Primary allocation in cylinders | | 420 | |
| Secondary allocation in cylinders | | 100 | |
| * If you select the zSeries File System, you might want to change the extension of this file to .ZFS. | | | |

Table 44. WebSphere Application Server Product File System.

Enter your values:

| Item | | Default | Your value |
|-------------------------------|---|--|------------|
| Product file system directory | | /usr/lpp/ zWebSphere/ V7R0 | |
| Intermediate symbolic link | | | |
| | Create intermediate symbolic link | Selected | |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ node_long_name/ wassmpe | |

Table 45. Feature Pack for SCA Product File System.

Enter your values:

| Item | | Default | Your value |
|-------------------------------|---|--|------------|
| Product file system directory | | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | | |
| | Create intermediate symbolic link | Selected | |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ node_long_name/ fpscasmpe | |

Table 46. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.5 or later, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

| Item | Default | Your value |
|--|-------------------|------------|
| Error log stream | | |
| Error log stream name (optional) | BBOCELL.ERROR.LOG | |
| CTRACE parmli member | | |
| CTRACE parmli member suffix (optional) | 60 | |

Table 47. Process Definitions.

Enter your values:

| Item | Default | Your value |
|--------------------|---------------------------|---------------------------|
| Controller process | | |
| Job name | <i>server_short_name</i> | <i>server_short_name</i> |
| Procedure name | BBO7DCR | |
| Servant process | | |
| Job name | <i>server_short_nameS</i> | <i>server_short_nameS</i> |
| Procedure name | BBO7DSR | |

Table 48. Port Values Assignment.

Enter your values:

| Item | Default | Your value |
|--|---------|------------|
| Node host name or IP address | | |
| None | | |
| JMX SOAP connector port | 8879 | |
| Cell discovery address port | 7277 | |
| ORB listener IP address | | |
| * | | |
| ORB port | 9809 | |
| ORB SSL port | 0 | |
| HTTP transport IP address | | |
| * | | |
| Administrative console port | 9060 | |
| Administrative console secure port | 9043 | |
| Administrative interprocess communication port (K) | 9632 | |
| High Availability Manager communication port (DCS) | 9352 | |

Table 48. Port Values Assignment (continued).

Enter your values:

| Item | Default | Your value |
|--|---------|------------|
| DataPower® appliance manager secure inbound port (Z) | 5555 | |

Table 49. Location Service Daemon Definitions.

Enter your values:

| Item | Default | Your value |
|------------------------------|---|--|
| Daemon home directory | /wasv7config/ cell_long_name/ node_long_name/Daemon | /wasv7config/cell_long_name/ node_long_name/Daemon |
| Daemon job name | BBODMNC | |
| Procedure name | BBO7DMNC | |
| IP name | host_name | |
| Listen IP | * | |
| Port | 5755 | |
| SSL port | 5756 | |
| Register daemon with WLM DNS | Not selected | |

Table 50. SSL Customization.

Enter your values:

| Item | Default | Your value |
|---|----------------------------|------------|
| Certificate authority keylabel | WebSphereCA | |
| Generate certificate authority (CA) certificate | Selected | |
| Expiration date for certificates | 2018/12/31 | |
| Default SAF keyring name | WASKeyring.cell_short_name | |
| Enable SSL on location service daemon | Selected | |

Table 51. Administrative Security Selection.

Enter your values:

| Item | Default | Your value |
|----------------------------------|--------------|------------|
| Use a z/OS security product | Selected | |
| Use WebSphere Application Server | Not selected | |
| Do not enable security | Not selected | |

Table 52. Security Managed by the z/OS Product.

Enter your values:

| Item | Default | Your value |
|---|---------------------------------|--------------|
| SAF profile prefix | <i>cell_short_name</i> | |
| WebSphere Application Server unauthenticated user | | |
| | User ID | WSGUEST |
| | Allow OS security to assign UID | Not selected |
| | Assign user-specified UID | Selected |
| | UID | 2402 |
| Enable writable SAF keyring support | Not selected | |

Table 53. Security Managed by the WebSphere Family Product.

Enter your values:

| Item | Default | Your value |
|-----------|---------|------------|
| User name | WSADMIN | |
| Password | None | |

Table 54. Security Certificate.

Enter your values:

| Item | Default | Your value |
|------------------------------|------------------------------|--|
| Default personal certificate | | |
| | Issued to distinguished name | <i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i> |
| | Issued by distinguished name | <i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i> |
| | Expiration period in years | 1 |
| Root signing certificate | | |
| | Expiration period in years | 20 |
| Default keystore password | | |

Table 55. Job Statement Definition.

Enter your values:

| Item | Default | Your value |
|---------------|---|------------|
| //jobname JOB | (ACCTNO,ROOM), 'USERID', CLASS=A, REGION=OM | |
| //* | //* | |
| //* | //* | |

Table 55. Job Statement Definition (continued).

Enter your values:

| Item | Default | Your value |
|------|---------|------------|
| //* | //* | |

Using the Profile Management Tool to enable existing z/OS deployment managers for the Feature Pack for SCA

You can use the Profile Management tool to enable the Feature Pack for SCA on an existing z/OS deployment manager. This topic includes steps to enable the Feature Pack for SCA on an existing deployment manager. When this task is complete, you can federate application servers that have been enabled for the feature pack into a Network Deployment cell.

Before you begin

Before starting this procedure, perform the following actions:

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, "Installing the Feature Pack for SCA Version 1.0 on z/OS systems," on page 17.
2. Install the workstation-based WebSphere Customization Tools, which include the Profile Management Tool.
3. Install the Feature Pack for SCA extension for the Profile Management Tool.
4. Select the deployment manager that you want to enable for the feature pack, and fill out a copy of the "z/OS augmentation worksheet: Deployment managers with the Feature Pack for SCA" on page 47.

1. Start the Profile Management Tool.
2. Create a customization definition for augmenting a profile with the Feature Pack for SCA.
For more information, read "z/OS augmentation worksheet: Deployment managers with the Feature Pack for SCA" on page 47.
 - a. In the **Customization Locations** table, select the location of the customization definition that you want to create.
 - b. Click the **Customization Definitions** tab if it is not already selected.
 - c. Click **Augment**.
 - d. Select **Management**.
 - e. Click **Next**.
 - f. Select **Management with Feature Pack for SCA Version 1.0**.
 - g. Click **Next**.
 - h. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

- i. Click **Augment**.
- j. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
 - If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.
3. Review the customization definition response file to confirm that the values are correct.
 4. Upload the customization jobs and instructions to the target z/OS system.
 5. Follow the generated instructions, which you can view using one of the following methods:
 - In the Profile Management Tool, select the desired customization definition and select the **Customization Instructions** tab.
 - After you upload the definition, view the IWODINSM job in the target CNTL dataset, which contains a text version of the instructions.
 6. If you encounter problems caused by your values in the customization definition, modify your variables using the Profile Management Tool, regenerate the instructions, and upload the customization definitions again.

Notes:

- Do not attempt to fix a typographical error or make a change by modifying the generated output. Many of the variables are used in multiple members of the target datasets; if you do not change them all, therefore, you might experience errors that are difficult to diagnose.
- Remember that you cannot upload new customization jobs while either configuration dataset is open.

Results

Your existing z/OS deployment manager is now enabled for the Feature Pack for SCA.

z/OS augmentation worksheet: Deployment managers with the Feature Pack for SCA

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this deployment manager:

System name: _____

Sysplex name: _____

Table 56. Customization Definition Name.

Enter your values:

| Item | Default | Your value |
|------------------------------------|---------------|------------|
| Customization definition name | ZSCAAugDMgrxx | |
| Response file path name (optional) | None | |

Table 57. Target Datasets.

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| High-level qualifier (HLQ) | None | |

Table 58. Base File Systems.

Enter your values:

| Item | Default | Your value |
|--|-------------------------------|------------|
| Configuration file system | | |
| Mount point | /wasv7config | |
| Directory path name relative to mount point | DeploymentManager | |
| WebSphere Application Server product file system | | |
| Product file system directory (or path name of intermediate symbolic link) | /usr/lpp/ zWebSphere/ V7R0 | |

Table 59. Feature Pack for SCA Product File System.

Enter your values:

| Item | Default | Your value |
|-------------------------------|--|----------------------------|
| Product file system directory | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | |
| | Create intermediate symbolic link | Selected |
| | Path name of intermediate symbolic link | /wasv7config/ fpscasmpe |

Table 60. Target Node Administrative Security.

Enter your values:

| Item | Default | Your value |
|---|-------------------------------|------------|
| Target node is managed by a z/OS security product | Selected | |
| | SAF profile prefix (optional) | None |

Table 61. Job Statement Definition.

Enter your values:

| Item | Default | Your value |
|---------------|---|------------|
| //jobname JOB | (ACCTNO,ROOM), 'USERID', CLASS=A,REGION=OM | |
| //* | //* | |
| //* | //* | |
| //* | //* | |

Using the Profile Management Tool to create z/OS managed (custom) nodes with the Feature Pack for SCA installed

You can use the Profile Management Tool to generate the jobs required to create a z/OS managed (custom) node with the Feature Pack for SCA installed.

Before you begin

Before starting this procedure, perform the following actions:

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, "Installing the Feature Pack for SCA Version 1.0 on z/OS systems," on page 17.
 2. Install the workstation-based WebSphere Customization Tools, which include the Profile Management Tool.
 3. Install the Feature Pack for SCA extension for the Profile Management Tool.
 4. Plan your managed (custom) node environment, and fill out a copy of the "z/OS customization worksheet: Managed (custom) nodes with the Feature Pack for SCA" on page 51.
1. Start the Profile Management Tool.
 2. Optional: If you want to add a customization location to the **Customization Locations** table, perform the following actions:
 - a. Click **Add**.
 - b. Enter the path name of the location where you want to store the customization definitions and associated data.

Important: The customization location directory must be empty when you create a new customization location.

- c. Perform one of the following actions:
 - If you want to use an existing customization location, select **Use an existing customization location**.
 - If you want to create a new customization location, select **Create a new customization location**.
Enter a value for the name that is meaningful to you, and select Version 7.0.
- d. Click **Finish**.
3. Create a customization definition that includes the Feature Pack for SCA.
For more information, read "z/OS customization worksheet: Managed (custom) nodes with the Feature Pack for SCA" on page 51.

- a. In the **Customization Locations** table, select the location of the customization definition that you want to create.
- b. Click the **Customization Definitions** tab if it is not already selected.
- c. Click **Create**.
- d. Expand **WebSphere Application Server Feature Pack for SCA Version 1.0**.
- e. Select **Managed (custom) node with Feature Pack for SCA Version 1.0**.
- f. Click **Next**.
- g. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

- h. Click **Create**.
- i. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
 - If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.
4. Review the managed (custom) node definition response file to confirm that the values are correct.
 5. Upload the customization jobs and instructions to the target z/OS system.
 6. Follow the generated instructions, which you can view using one of the following methods:
 - In the Profile Management Tool, select the desired customization definition and select the **Customization Instructions** tab.
 - After you upload the definition, view member BBOMNINS in the target CNTL dataset, which will be identified on the upload panel.
 7. If you encounter problems caused by your values in the customization definition, modify your variables using the Profile Management Tool, regenerate the instructions, and upload the customization definitions again.

Notes:

- Do not attempt to fix a typographical error or make a change by modifying the generated output. Many of the variables are used in multiple members of the target datasets; if you do not change them all, therefore, you might experience errors that are difficult to diagnose.
- Remember that you cannot upload new customization jobs while either configuration dataset is open.

Results

You have set up a new z/OS managed (custom) node with the Feature Pack for SCA installed.

z/OS customization worksheet: Managed (custom) nodes with the Feature Pack for SCA

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this managed (custom) node:

System name: _____

Sysplex name: _____

Table 62. Customization Definition Name.

Enter your values:

| Item | Default | Your value |
|------------------------------------|--------------|------------|
| Customization definition name | ZSCACustomxx | |
| Response file path name (optional) | None | |

Table 63. Default Values.

Enter your values:

| Item | Default | Your value |
|---|--------------|------------|
| GID and UID defaults | | |
| Set each default GID and UID value to indicate OS security is to assign an unused value | Not selected | |
| Name and userid defaults | | |
| Set default names and userids based on cell and system identifiers | Not selected | |
| Two-character cell identifier | AZ | |
| Single-character system identifier | A | |
| Port defaults | | |
| Set default port values from the following port range | Not selected | |
| Lowest default port number | 9550 | |
| Highest default port number | 9559 | |

Table 64. Target Datasets.

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| High-level qualifier (HLQ) | None | |

Table 65. Configure Common Groups.

Enter your values:

| Item | Default | Your value |
|--|--------------|------------|
| WebSphere Application Server configuration group information | | |
| Group | WSCFG1 | |
| Allow OS security to assign GID | Not selected | |
| Assign user-specified GID | Selected | |
| Specified GID | 2500 | |
| WebSphere Application Server servant group information | | |
| Group | WSSR1 | |
| Allow OS security to assign GID | Not selected | |
| Assign user-specified GID | Selected | |
| Specified GID | 2501 | |
| WebSphere Application Server local user group information | | |
| Group | WSCLGP | |
| Allow OS security to assign GID | Not selected | |
| Assign user-specified GID | Selected | |
| Specified GID | 2502 | |

Table 66. Configure Common Users.

Enter your values:

| Item | Default | Your value |
|--|--------------|------------|
| Common controller user ID | | |
| User ID | WSCRU1 | |
| Allow OS security to assign UID | Not selected | |
| Assign user-specified UID | Selected | |
| Specified UID | 2431 | |
| Common servant user ID | | |
| User ID | WSSRU1 | |
| Allow OS security to assign UID | Not selected | |
| Assign user-specified UID | Selected | |
| Specified UID | 2432 | |
| WebSphere Application Server administrator | | |

Table 66. Configure Common Users (continued).

Enter your values:

| Item | | Default | Your value |
|---|---------|---------------------------------|--------------|
| | User ID | WSADMIN | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2403 |
| Asynchronous administration user ID | | | |
| | User ID | WSADMSH | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2504 |
| WebSphere Application Server user ID home directory | | /var/ WebSphere/ home | |

Table 67. Configure Additional Users.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.1 or later, select **Enable unique user IDs for daemon and adjunct**, and click **Apply**.

Enter your values:

| Item | | Default | Your value |
|----------------------------|---------|---------------------------------|--------------|
| Controller adjunct user ID | | | |
| | User ID | WSCRAU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2433 |
| Daemon user ID | | | |
| | User ID | WSDMNU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2434 |

Table 68. System and Dataset Names.

Enter your values:

| Item | Default | Your value |
|----------------------|--------------|------------|
| System name | None | |
| Sysplex name | None | |
| PROCLIB dataset name | SYS1.PROCLIB | |

Table 69. Node Names.

Enter your values:

| Item | Default | Your value |
|------------|---------|------------|
| Node names | | |
| Short name | BBONODE | |
| Long name | bbonode | |

Table 70. Configuration File System.

Enter your values:

| Item | Default | Your value |
|---|--|--------------|
| Mount point | /wasv7config/ cell_long_name/ node_long_name | |
| Directory path name relative to mount point | AppServer | |
| Dataset name | OMVS.WAS70. cell_short_name. node_short_name.HFS * | |
| File system type | | |
| | Hierarchical File System (HFS) | Selected |
| | zSeries File System (ZFS) | Not selected |
| Volume, or '*' for SMS | * | |
| Primary allocation in cylinders | 300 | |
| Secondary allocation in cylinders | 100 | |
| * If you select the zSeries File System, you might want to change the extension of this file to .ZFS. | | |

Table 71. WebSphere Application Server Product File System.

Enter your values:

| Item | Default | Your value |
|-------------------------------|---|--|
| Product file system directory | /usr/lpp/ zWebSphere/ V7R0 | |
| Intermediate symbolic link | | |
| | Create intermediate symbolic link | Selected |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ node_long_name/ wassmpe |

Table 72. Feature Pack for SCA Product File System.

Enter your values:

| Item | Default | Your value |
|-------------------------------|--|--|
| Product file system directory | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | |
| | Create intermediate symbolic link | Selected |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ node_long_name/ fpscasmpe |

Table 73. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.5 or later, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

| Item | Default | Your value |
|----------------------|--|-------------------|
| Error log stream | | |
| | Error log stream name (optional) | BBOCELL.ERROR.LOG |
| CTRACE parmli member | | |
| | CTRACE parmli member suffix (optional) | 60 |

Table 74. Process Definitions.

Enter your values:

| Item | Default | Your value |
|--|----------------|------------|
| Controller process | | |
| | Procedure name | BBO7ACR |
| Controller adjunct process | | |
| | Procedure name | BBO7CRA |
| Servant process | | |
| | Procedure name | BBO7ASR |
| Admin asynch operations procedure name | | |
| | | BBO7ADM |

Table 75. Location Service Daemon Definitions.

Enter your values:

| Item | Default | Your value |
|-----------------------|---|---|
| Daemon home directory | /wasv7config/ cell_long_name/ node_long_name/Daemon | /wasv7config/cell_long_name/ node_long_name/Daemon |

Table 75. Location Service Daemon Definitions (continued).

Enter your values:

| Item | Default | Your value |
|-----------------|----------|------------|
| Daemon job name | BBODMNB | |
| Procedure name | BBO7DMNB | |

Table 76. SSL Customization.

Enter your values:

| Item | Default | Your value |
|----------------------------------|----------------------------|------------|
| Certificate authority keylabel | WebSphereCA | |
| Expiration date for certificates | 2018/12/31 | |
| Default SAF keyring name | WASKeyring.cell_short_name | |

Table 77. Administrative Security Selection.

Enter your values:

| Item | Default | Your value |
|----------------------------------|--------------|------------|
| Use a z/OS security product | Selected | |
| Use WebSphere Application Server | Not selected | |
| Do not enable security | Not selected | |

Table 78. Federate Application Server (Part 1).

Enter your values:

| Item | Default | Your value |
|---------------------------|---|--|
| Application server access | | |
| | WebSphere Application Server home directory path name | |
| | Configuration file system mount point | /wasv7config/ cell_long_name/ node_long_name |
| | Directory path name relative to mount point | AppServer |
| Deployment manager access | | |

Table 78. Federate Application Server (Part 1) (continued).

Enter your values:

| Item | Default | Your value |
|---|--------------|------------|
| Node host name or IP address | None | |
| Deployment manager JMX connection type | | |
| RMI | Not selected | |
| SOAP | Selected | |
| Deployment manager JMX port | 8879 | |
| Deployment manager connection requires security information | Not selected | |
| User ID | WSADMIN | |
| Password | None | |

Table 79. Federate Application Server (Part 2).

Enter your values:

| Item | Default | Your value |
|--|------------------|------------|
| Node agent definitions | | |
| Server name (short) | BBON001 | |
| Server name (long) | nodeagent | nodeagent |
| Node host name | None | |
| JMX SOAP connector port | 8878 | |
| ORB listener IP address | * | |
| ORB port | 2810 | |
| ORB SSL port | 0 | |
| Node discovery port | 7272 | |
| Node multicast discovery port | 5000 | |
| Node IPv6 multicast discovery port | 5001 | |
| Administrative local port | 9626 | |
| High Availability Manager communication port (DCS) | 9354 | |
| Node group name | DefaultNodeGroup | |
| Launch the node agent after federation | Selected | |
| Enable writable SAF keyring support | Not selected | |

Table 80. Security Certificate.

Enter your values:

| Item | Default | Your value |
|------------------------------|---------|------------|
| Default personal certificate | | |

Table 80. Security Certificate (continued).

Enter your values:

| Item | | Default | Your value |
|---------------------------|------------------------------|---|------------|
| | Issued to distinguished name | cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US | |
| | Issued by distinguished name | cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US | |
| | Expiration period in years | 1 | |
| Root signing certificate | | | |
| | Expiration period in years | 20 | |
| Default keystore password | | | |

Table 81. Job Statement Definition.

Enter your values:

| Item | Default | Your value |
|---------------|--|------------|
| //jobname JOB | (ACCTNO,ROOM),'USERID', CLASS=A,REGION=OM | |
| //* | //* | |
| //* | //* | |
| //* | //* | |

Using the Profile Management Tool to enable existing z/OS managed (custom) nodes for the Feature Pack for SCA

You can use the Profile Management Tool to enable the Feature Pack for SCA on an existing z/OS managed (custom) node.

Before you begin

Before starting this procedure, perform the following actions:

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, "Installing the Feature Pack for SCA Version 1.0 on z/OS systems," on page 17.
 2. Install the workstation-based WebSphere Customization Tools, which include the Profile Management Tool.
 3. Install the Feature Pack for SCA extension for the Profile Management Tool.
 4. Select the managed (custom) node that you want to enable for the feature pack, and fill out a copy of the "z/OS augmentation worksheet: Managed (custom) nodes with the Feature Pack for SCA" on page 60.
1. Start the Profile Management Tool.

2. Create a customization definition for augmenting a profile with the Feature Pack for SCA.

For more information, read “z/OS augmentation worksheet: Managed (custom) nodes with the Feature Pack for SCA” on page 60.

- a. In the **Customization Locations** table, select the location of the customization definition that you want to create.
- b. Click the **Customization Definitions** tab if it is not already selected.
- c. Click **Augment**.
- d. Select **Managed (custom) node**.
- e. Click **Next**.
- f. Select **Managed (custom) node with Feature Pack for SCA Version 1.0**.
- g. Click **Next**.
- h. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

- i. Click **Augment**.
- j. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
- If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.

3. Review the customization definition response file to confirm that the values are correct.
4. Upload the customization jobs and instructions to the target z/OS system.
5. Follow the generated instructions, which you can view using one of the following methods:
 - In the Profile Management Tool, select the desired customization definition and select the **Customization Instructions** tab.
 - After you upload the definition, view the IWODINSN job in the target CNTL dataset, which contains a text version of the instructions.
6. If you encounter problems caused by your values in the customization definition, modify your variables using the Profile Management Tool, regenerate the instructions, and upload the customization definitions again.

Notes:

- Do not attempt to fix a typographical error or make a change by modifying the generated output. Many of the variables are used in

multiple members of the target datasets; if you do not change them all, therefore, you might experience errors that are difficult to diagnose.

- Remember that you cannot upload new customization jobs while either configuration dataset is open.

Results

Your existing WebSphere Application Server for z/OS managed (custom) node is enabled for the Feature Pack for SCA.

z/OS augmentation worksheet: Managed (custom) nodes with the Feature Pack for SCA

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this managed (custom) node:

System name: _____

Sysplex name: _____

Table 82. Customization Definition Name.

Enter your values:

| Item | Default | Your value |
|------------------------------------|-----------------|------------|
| Customization definition name | ZSCAAugCustomxx | |
| Response file path name (optional) | None | |

Table 83. Target Datasets.

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| High-level qualifier (HLQ) | None | |

Table 84. Base File Systems.

Enter your values:

| Item | Default | Your value |
|--|-------------------------------|------------|
| Configuration file system | | |
| Mount point | /wasv7config | |
| Directory path name relative to mount point | AppServer | |
| WebSphere Application Server product file system | | |
| Product file system directory (or path name of intermediate symbolic link) | /usr/lpp/ zWebSphere/ V7R0 | |

Table 85. Feature Pack for SCA Product File System.

Enter your values:

| Item | Default | Your value |
|-------------------------------|--|----------------------------|
| Product file system directory | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | |
| | Create intermediate symbolic link | Selected |
| | Path name of intermediate symbolic link | /wasv7config/ fpscasmpe |

Table 86. Target Node Administrative Security.

Enter your values:

| Item | Default | Your value |
|---|-------------------------------|------------|
| Target node is managed by a z/OS security product | Selected | |
| | SAF profile prefix (optional) | None |

Table 87. Job Statement Definition.

Enter your values:

| Item | Default | Your value |
|---------------|---|------------|
| //jobname JOB | (ACCTNO,ROOM), 'USERID', CLASS=A,REGION=OM | |
| //* | //* | |
| //* | //* | |
| //* | //* | |

Using the Profile Management Tool to create z/OS Network Deployment cells with the Feature Pack for SCA installed

You can use the Profile Management Tool to generate the jobs required to create a z/OS Network Deployment cell with the Feature Pack for SCA installed.

Before you begin

The cell set of profiles that you create using this procedure might not be appropriate for use in production environments. You might not be able to augment the deployment manager and application server profiles created from this template with additional features or capabilities after they are created. If this is a concern, create a management profile with a deployment manager and then build out the cell by federating application servers to the deployment manager.

Before starting this procedure, perform the following actions:

1. Install the feature-pack code on the target z/OS system.

For more information, read Chapter 4, “Installing the Feature Pack for SCA Version 1.0 on z/OS systems,” on page 17.

2. Install the workstation-based WebSphere Customization Tools, which include the Profile Management Tool.
3. Install the Feature Pack for SCA extension for the Profile Management Tool.
4. Plan your Network Deployment environment, and fill out a copy of the “z/OS customization worksheet: Network Deployment cells with the Feature Pack for SCA” on page 63.

1. Start the Profile Management Tool.
2. Optional: If you want to add a customization location to the **Customization Locations** table, perform the following actions:
 - a. Click **Add**.
 - b. Enter the path name of the location where you want to store the customization definitions and associated data.

Important: The customization location directory must be empty when you create a new customization location.

- c. Perform one of the following actions:
 - If you want to use an existing customization location, select **Use an existing customization location**.
 - If you want to create a new customization location, select **Create a new customization location**.
Enter a value for the name that is meaningful to you, and select Version 7.0.
- d. Click **Finish**.
3. Create a customization definition that includes the Feature Pack for SCA.
For more information, read “z/OS customization worksheet: Network Deployment cells with the Feature Pack for SCA” on page 63.
 - a. In the **Customization Locations** table, select the location of the customization definition that you want to create.
 - b. Click the **Customization Definitions** tab if it is not already selected.
 - c. Click **Create**.
 - d. Expand **WebSphere Application Server Feature Pack for SCA Version 1.0**.
 - e. Select **Cell with Feature Pack for SCA Version 1.0**.
 - f. Click **Next**.
 - g. Complete the fields in the panels using the configuration values that you entered for the variables on the configuration worksheet that you created, clicking **Back** and **Next** as necessary.

Tips:

- Hover your cursor over a field for help information.
- Click **Cancel** at any time to leave the creation process without generating a customization definition.

When you have successfully entered all of the necessary information on the panels for this type of customization definition, the Profile Management Tool displays the definition type, location, and name on the **Customization Summary** panel.

- h. Click **Create**.
- i. Click **Finish**.

Tips:

- You might want to make a note of the customization definition name and response-file location for future reference.
 - If you just make note of the name, you can get the response file location later from the **Customization Summary** panel after you select the customization definition name.
4. Review the cell definition response file to confirm that the values are correct.
 5. Upload the customization jobs and instructions to the target z/OS system.
 6. Follow the generated instructions, which you can view using one of the following methods:
 - In the Profile Management Tool, select the desired customization definition and select the **Customization Instructions** tab.
 - After you upload the definition, view member BBODMINS in the target CNTL dataset, which will be identified on the upload panel.
 7. If you encounter problems caused by your values in the customization definition, modify your variables using the Profile Management Tool, regenerate the instructions, and upload the customization definitions again.

Notes:

- Do not attempt to fix a typographical error or make a change by modifying the generated output. Many of the variables are used in multiple members of the target datasets; if you do not change them all, therefore, you might experience errors that are difficult to diagnose.
- Remember that you cannot upload new customization jobs while either configuration dataset is open.

Results

You have set up a new z/OS Network Deployment cell with the Feature Pack for SCA installed.

z/OS customization worksheet: Network Deployment cells with the Feature Pack for SCA

Print this worksheet, and use it when collecting information about the customization variables. The variables and defaults are provided along with spaces for you to fill in your own value for each.

Date: _____

Purpose of this cell:

System name: _____

Sysplex name: _____

Table 88. Customization Definition Name.

Enter your values:

| Item | Default | Your value |
|-------------------------------|------------|------------|
| Customization definition name | ZSCACellxx | |

Table 88. Customization Definition Name (continued).

Enter your values:

| Item | Default | Your value |
|------------------------------------|---------|------------|
| Response file path name (optional) | None | |

Table 89. Default Values.

Enter your values:

| Item | Default | Your value |
|--------------------------|---|--------------|
| GID and UID defaults | | |
| | Set each default GID and UID value to indicate OS security is to assign an unused value | Not selected |
| Name and userid defaults | | |
| | Set default names and userids based on cell, cluster, and system identifiers | Not selected |
| | Two-character cell identifier | AZ |
| | Two-character cluster identifier | 00 |
| | Single-character system identifier | A |
| Port defaults | | |
| | Set default port values from the following port range | Not selected |
| | Lowest default port number | 9510 |
| | Highest default port number | 9559 |

Table 90. Target Datasets.

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| High-level qualifier (HLQ) | None | |

Table 91. Configure Common Groups.

Enter your values:

| Item | Default | Your value |
|--|---------------------------------|--------------|
| WebSphere Application Server configuration group information | | |
| | Group | WSCFG1 |
| | Allow OS security to assign GID | Not selected |
| | Assign user-specified GID | Selected |
| | Specified GID | 2500 |
| WebSphere Application Server servant group information | | |

Table 91. Configure Common Groups (continued).

Enter your values:

| Item | | Default | Your value |
|---|-------|---------------------------------|--------------|
| | Group | WSSR1 | |
| | | Allow OS security to assign GID | Not selected |
| | | Assign user-specified GID | Selected |
| | | Specified GID | 2501 |
| WebSphere Application Server local user group information | | | |
| | Group | WSCLGP | |
| | | Allow OS security to assign GID | Not selected |
| | | Assign user-specified GID | Selected |
| | | Specified GID | 2502 |

Table 92. Configure Common Users.

Enter your values:

| Item | | Default | Your value |
|---|---------|---------------------------------|--------------|
| Common controller user ID | | | |
| | User ID | WSCRUI | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2431 |
| Common servant user ID | | | |
| | User ID | WSSRU1 | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2432 |
| WebSphere Application Server administrator | | | |
| | User ID | WSADMIN | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2403 |
| Asynchronous administration user ID | | | |
| | User ID | WSADMSH | |
| | | Allow OS security to assign UID | Not selected |
| | | Assign user-specified UID | Selected |
| | | Specified UID | 2504 |
| WebSphere Application Server user ID home directory | | /var/ WebSphere/ home | |

Table 93. System and Dataset Names.

Enter your values:

| Item | Default | Your value |
|----------------------|--------------|------------|
| System name | None | |
| Sysplex name | None | |
| PROCLIB dataset name | SYS1.PROCLIB | |

Table 94. Cell, Node, and Server Names.

Enter your values:

| Item | Default | Your value |
|--|------------|--------------|
| Cell names | | |
| | Short name | BBOCELL |
| | Long name | bbocell |
| Deployment manager node names | | |
| | Short name | BBODMGR |
| | Long name | bbodmgr |
| Deployment manager server names | | |
| | Short name | BBODMGR |
| | Long name | dmgr |
| Node agent and application server node names | | |
| | Short name | BBONODE |
| | Long name | bbonode |
| Node agent server names | | |
| | Short name | BBON001 |
| | Long name | nodeagent |
| Application server names | | |
| | Short name | BBOS001 |
| | Long name | server1 |
| Deployment manager cluster transition name | BBODMGR | |
| Application server cluster transition name | BBOC001 | |
| JVM mode | | |
| | 31 bit | Not selected |
| | 64 bit | Selected |

Table 95. Deployment Manager Configuration File System.

Enter your values:

| Item | Default | Your value |
|---|--|------------|
| Mount point | /wasv7config/ cell_long_name/ node_long_name | |
| Directory path name relative to mount point | DeploymentManager | |

Table 95. Deployment Manager Configuration File System (continued).

Enter your values:

| Item | | Default | Your value |
|---|--------------------------------|--|------------|
| Dataset name | | OMVS.WAS70. <i>cell_short_name</i> . <i>node_short_name</i> .HFS * | |
| File system type | | | |
| | Hierarchical File System (HFS) | Selected | |
| | zSeries File System (ZFS) | Not selected | |
| Volume, or '*' for SMS | | * | |
| Primary allocation in cylinders | | 420 | |
| Secondary allocation in cylinders | | 100 | |
| * If you select the zSeries File System, you might want to change the extension of this file to .ZFS. | | | |

Table 96. Deployment Manager Product File System.

Enter your values:

| Item | | Default | Your value |
|-------------------------------|---|--|------------|
| Product file system directory | | /usr/lpp/ zWebSphere/ V7R0 | |
| Intermediate symbolic link | | | |
| | Create intermediate symbolic link | Selected | |
| | Path name of intermediate symbolic link | /wasv7config/ <i>cell_long_name</i> / <i>node_long_name</i> / wassmpe | |

Table 97. Feature Pack for SCA Deployment Manager Product File System.

Enter your values:

| Item | | Default | Your value |
|-------------------------------|---|--|------------|
| Product file system directory | | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | | |
| | Create intermediate symbolic link | Selected | |
| | Path name of intermediate symbolic link | /wasv7config/ <i>cell_long_name</i> / <i>node_long_name</i> / fpscasmpe | |

Table 98. Application Server Configuration File System.

Enter your values:

| Item | Default | Your value |
|---|--|--------------|
| Mount point | /wasv7config/ cell_long_name/ node_long_name | |
| Directory path name relative to mount point | AppServer | |
| Dataset name | OMVS.WAS70. cell_short_name. node_short_name.HFS | |
| File system type | | |
| | Hierarchical File System (HFS) | Selected |
| | zSeries File System (ZFS) | Not selected |
| Volume, or '*' for SMS | * | |
| Primary allocation in cylinders | 420 | |
| Secondary allocation in cylinders | 100 | |

Table 99. Application Server Product File System.

Enter your values:

| Item | Default | Your value |
|-------------------------------|---|---|
| Product file system directory | /usr/lpp/ zWebSphere/ V7R0 | |
| Intermediate symbolic link | | |
| | Create intermediate symbolic link | Selected |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ nodeagent_long_name/ wassmpe |

Table 100. Feature Pack for SCA Application Server Product File System.

Enter your values:

| Item | Default | Your value |
|-------------------------------|--|--|
| Product file system directory | /usr/lpp/ zWebSphere_OM/ V7R0/ FPSCA | |
| Intermediate symbolic link | | |
| | Create intermediate symbolic link | Selected |
| | Path name of intermediate symbolic link | /wasv7config/ cell_long_name/ node_long_name/ fpscasmpe |

Table 101. Error Log Stream and CTRACE Parmlib Member.

This panel only displays if you click **Window > Preferences > Profile Management Tool** in WebSphere Customization Tools Version 7.0.0.5 or later, select **Enable error log stream and CTRACE parmli member**, and click **Apply**. Alternatively, you can use the administrative console to set these values.

Enter your values:

| Item | Default | Your value |
|--|-------------------|------------|
| Error log stream | | |
| Error log stream name (optional) | BBOCELL.ERROR.LOG | |
| CTRACE parmli member | | |
| CTRACE parmli member suffix (optional) | 60 | |

Table 102. Optional Application Deployment.

Enter your values:

| Item | Default | Your value |
|-----------------------------------|--------------|------------|
| Deploy the administrative console | Selected | |
| Deploy the default application | Selected | |
| Deploy the sample applications | Not selected | |

Table 103. Process Definitions.

Enter your values:

| Item | Default | Your value |
|---|---------------------------|---------------------------|
| Deployment manager controller process | | |
| Job name | <i>server_short_name</i> | <i>server_short_name</i> |
| Procedure name | BBO7DCR | |
| Deployment manager servant process | | |
| Job name | <i>server_short_nameS</i> | <i>server_short_nameS</i> |
| Procedure name | BBO7DSR | |
| Application server controller process | | |
| Job name | <i>server_short_name</i> | <i>server_short_name</i> |
| Procedure name | BBO7ACR | |
| Application server controller adjunct process | | |
| Job name | <i>server_short_nameA</i> | <i>server_short_nameA</i> |
| Procedure name | BBO7CRA | |
| Application server servant process | | |
| Job name | <i>server_short_nameS</i> | <i>server_short_nameS</i> |
| Procedure name | BBO7ASR | |
| Admin asynch operations procedure name | BBO7ADM | |

Table 104. Port Values Assignment.

Enter your values:

| Item | Default | Your value |
|---|---------|------------|
| Deployment manager ports | | |
| Node host name or IP address | None | |
| JMX SOAP connector port | 8879 | |
| Cell discovery address port | 7277 | |
| ORB listener IP address | * | |
| ORB port | 9809 | |
| ORB SSL port | 0 | |
| HTTP transport IP address | * | |
| Administrative console port | 9060 | |
| Administrative console secure port | 9043 | |
| Administrative interprocess communication port (K) | 9632 | |
| High Availability Manager communication port (DCS) | 9352 | |
| DataPower appliance manager secure inbound port (Z) | 5555 | |
| Node agent ports | | |
| JMX SOAP connector port | 8878 | |
| ORB port | 2810 | |
| ORB SSL port | 0 | |
| Node agent interprocess communication port (K) | 9626 | |
| High Availability Manager communication port (DCS) | 9354 | |
| Node discovery port | 7272 | |
| Node multicast discovery port | 5000 | |
| Node IPv6 multicast discovery port | 5001 | |
| Application server ports | | |
| JMX SOAP connector port | 8880 | |
| ORB port | 2809 | |
| ORB SSL port | 0 | |
| HTTP transport port | 9080 | |
| HTTPS transport port | 9443 | |
| Administrative local port | 9633 | |
| High Availability Manager communication port (DCS) | 9353 | |

Table 104. Port Values Assignment (continued).

Enter your values:

| Item | Default | Your value |
|---|---------|------------|
| Service integration port | 7276 | |
| Service integration secure port | 7286 | |
| Service integration MQ interoperability port | 5558 | |
| Service integration MQ interoperability secure port | 5578 | |
| Session initiation protocol (SIP) port | 5060 | |
| Session initiation protocol (SIP) secure port | 5061 | |

Table 105. Location Service Daemon Definitions.

Enter your values:

| Item | Default | Your value |
|------------------------------|--|--|
| Daemon home directory | /wasv7config/ cell_long_name/ dngr_node_long_name/ Daemon | /wasv7config/cell_long_name/ dngr_node_long_name/ Daemon |
| Daemon job name | BBODMNC | |
| Procedure name | BBO7DMNC | |
| IP name | host_name | |
| Listen IP | * | |
| Port | 5755 | |
| SSL port | 5756 | |
| Register daemon with WLM DNS | Not selected | |

Table 106. SSL Customization.

Enter your values:

| Item | Default | Your value |
|---|----------------------------|------------|
| Certificate authority keylabel | WebSphereCA | |
| Generate certificate authority (CA) certificate | Selected | |
| Expiration date for certificates | 2018/12/31 | |
| Default SAF keyring name | WASKeyring.cell_short_name | |
| Enable SSL on location service daemon | Selected | |

Table 107. Administrative Security Selection.

Enter your values:

| Item | Default | Your value |
|----------------------------------|--------------|------------|
| Use a z/OS security product | Selected | |
| Use WebSphere Application Server | Not selected | |
| Do not enable security | Not selected | |

Table 108. Security Managed by the z/OS Product.

Enter your values:

| Item | Default | Your value |
|---|---------------------------------|--------------|
| SAF profile prefix | <i>cell_short_name</i> | |
| WebSphere Application Server unauthenticated user | | |
| | User ID | WSGUEST |
| | Allow OS security to assign UID | Not selected |
| | Assign user-specified UID | Selected |
| | UID | 2402 |
| Enable writable SAF keyring support | Not selected | |

Table 109. Security Managed by the WebSphere Family Product.

Enter your values:

| Item | Default | Your value |
|---------------------|-----------|------------|
| User name | WSADMIN | |
| Password | None | |
| Sample applications | | |
| | User name | samples |
| | Password | None |

Table 110. Security Certificate.

Enter your values:

| Item | Default | Your value |
|------------------------------|------------------------------|--|
| Default personal certificate | | |
| | Issued to distinguished name | <i>cn=host_name, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i> |
| | Issued by distinguished name | <i>cn=host_name, ou=Root Certificate, ou=cell_short_name, ou=node_short_name, o=IBM,c=US</i> |
| | Expiration period in years | 1 |

Table 110. Security Certificate (continued).

Enter your values:

| Item | Default | Your value |
|----------------------------|---------|------------|
| Root signing certificate | | |
| Expiration period in years | 25 | |
| Default keystore password | | |

Table 111. Web Server Definition (Part 1).

Enter your values:

| Item | Default | Your value |
|------------------------------------|------------------|--------------|
| Create a Web server definition | | Not selected |
| Web server type | IBM HTTP Server | |
| Web server operating system | z/OS | |
| Web server name | webserver1 | |
| Web server host name or IP address | <i>host_name</i> | |
| Web server port | 80 | |

Table 112. Web Server Definition (Part 2).

Enter your values:

| Item | Default | Your value |
|--|----------------------|------------|
| Web server installation directory path | /etc/websrv1 | |
| Web server plug-in installation directory path | /etc/websrv1/Plugins | |

Table 113. Job Statement Definition.

Enter your values:

| Item | Default | Your value |
|---------------|---|------------|
| //jobname JOB | (ACCTNO,ROOM), 'USERID', CLASS=A, REGION=OM | |
| //* | //* | |
| //* | //* | |
| //* | //* | |

Configuring with the zpmt command

Use the zpmt command to generate the customization definitions for creating new profiles with the feature pack installed and enabling existing profiles for the feature pack.

About this task

The `zpmt` command is an alternative to the workstation-based Profile Management Tool, which is launched from the WebSphere Customization Tools. You can use this command if you do not have a Windows or Linux workstation available to run the WebSphere Customization Tools or if you need to automate the generation of the WebSphere for z/OS customization jobs. You launch this command on the z/OS system that you need to configure using a shell script.

WebSphere Application Server for z/OS application serving environment nodes are created using batch jobs that are built with the Profile Management Tool or the `zpmt` command. After the node is configured and running, make further changes using the administrative console or scripting tool.

After you have installed the WebSphere Application Server for z/OS product, prepared your z/OS target systems, and planned your WebSphere Application Server for z/OS environment, perform the tasks in this section to configure needed response files.

1. Install the feature-pack code on the target z/OS system.
For more information, read Chapter 4, “Installing the Feature Pack for SCA Version 1.0 on z/OS systems,” on page 17.
2. Follow the directions for the type of response file that you want to configure. If you have already prepared a response file, proceed to the next step.
 - If you are creating a new standalone application server with the feature pack installed, refer to the list of variables and definitions in “Variables for using the `zpmt` command to create z/OS standalone application servers with the feature pack installed” on page 77.
 - If you are augmenting an existing standalone application server for the feature pack, refer to the list of variables and definitions in “Variables for using the `zpmt` command to enable existing z/OS standalone application servers for the feature pack” on page 90.
 - If you are creating a new deployment manager with the feature pack installed, refer to the list of variables and definitions in “Variables for using the `zpmt` command to create z/OS deployment managers with the feature pack installed” on page 92.
 - If you are augmenting an existing deployment manager for the feature pack, refer to the list of variables and definitions in “Variables for using the `zpmt` command to enable existing z/OS deployment managers for the feature pack” on page 103.
 - If you are creating a new managed (custom) node with the feature pack installed, refer to the list of variables and definitions in “Variables for using the `zpmt` command to create z/OS managed (custom) nodes with the feature pack installed” on page 106.
 - If you are augmenting an existing managed (custom) node for the feature pack, refer to the list of variables and definitions in “Variables for using the `zpmt` command to enable existing z/OS managed (custom) nodes for the feature pack” on page 116.
 - If you are creating a new Network Deployment cell with the feature pack installed, refer to the list of variables and definitions in “Variables for using the `zpmt` command to create z/OS Network Deployment cells with the feature pack installed” on page 119.
3. On your target z/OS system, run the `zpmt.sh` shell script using your prepared response file.

This tool creates the .CNTL and .DATA files needed to run the required jobs. The response file needs to be located in the UNIX[®] (USS) file system.

Important: The first time that you run the zpmt command, you must install the feature-pack extension for the command. The feature-pack extension is contained in the util/WCT directory within the SMP/E installation image of the feature pack. Run the zpmt command using the -installExtension argument to specify the path name of the SMP/E installation image. This causes the zpmt command to add the extension to its configuration. For example:

```
zpmt.sh -workspace eclipse_workspace_dir -responseFile response_file -allocate  
-transfer -replace -installExtension feature_pack_install_root
```

Once added, the support for the feature pack remains for subsequent zpmt invocations until the -uninstallExtension argument is used to remove the extension from the zpmt configuration. Note that there is also a -listExtensions argument for listing the configured extensions.

4. Follow the instructions in the xxxxxINS member of the .CNTL data to create the application serving environment.

zpmt command

The zpmt command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring the WebSphere Application Server for z/OS product.

Running the shell script

The zpmt.sh shell script is located in the *smpe_install_root/bin* or *was_home/bin* directory.

Definition of shell script syntax

These three attributes need a dataset or path following to be complete.

-responseFile

Specifies the path to your response file

-profilePath

Specifies a fully qualified path name to an existing set of generated jobs

This parameter cannot be used in combination with the -responsefile option.

-workspace

Specifies the Eclipse workspace directory

-transfer

Copies generated jobs from a UNIX System Services (USS) file system to a pair of partitioned datasets

The zpmt command first writes the customization jobs to a USS file system.

-allocate

Attempts to allocate the target datasets

This parameter cannot be used without the -transfer option.

-installExtension

Installs a feature-pack or stacked-product extension

This must include the absolute path name of the SMP/E installation root for a stacked product or feature pack. Using this parameter extracts the contents of the WebSphere Configuration Tool archive file contained within the specified installation file system and installs its contents into the Eclipse workspace directory

-listExtensions

Lists the extensions that are currently installed in the specified Eclipse workspace directory

-uninstallExtension

Removes the specified extension from the specified Eclipse workspace directory

-version

Version number of the extension to uninstall

Use this parameter to uninstall a specific version of an extension.

Datasets are determined by appending the values ".CNTL" and ".DATA" to the zTargetHLQ value for the profile containing the jobs that are being copied. This operation overwrites existing files of the same name in those datasets.

Sample syntax

The following examples describe typical command lines with attributes for the zpmt command. In these examples, /xxx can be any directory to which the user invoking zpmt.sh has read and write access.

- `zpmt.sh -workspace /xxx -transfer -allocate -responseFile /xxx/ZCellcmd.responseFile`

This does the following:

- Generates the customization jobs to the location specified by profilePath in the response file
- Allocates the target CNTL and DATA datasets using the high-level qualifier specified by targetHLQ in the response file
- Transfers the jobs from the file system to the CNTL and DATA data sets

- `zpmt.sh -workspace /xxx -responseFile /xxx/ZAppSrvcmd.responseFile`

This generates the customization jobs to the location specified by profilePath in the response file.

- `zpmt.sh -workspace /xxx -allocate -transfer -profilePath /xxx/ZAppSrvcmd`

This does the following:

- Allocates the target CNTL and DATA datasets using the high-level qualifier specified by targetHLQ in the response file
- Transfers the generated jobs at the location specified by -profilePath to those datasets

Note: This usage assumes the jobs have already been generated with a previous invocation of zpmt.sh.

- `zpmt.sh -workspace /xxx -transfer -responseFile /xxx/ZDmgcmd.responseFile`

This transfers the generated jobs from location profilePath in the response file to the generated CNTL and DATA datasets.

Note: This usage assumes that the jobs have already been generated with a previous invocation of `zpmc.sh` and that the target CNTL and DATA datasets have already been allocated

- `zpmc.sh -workspace eclipse_workspace_dir -responseFile response_file -allocate -transfer -replace -installExtension stacked_product_or_feature_pack_install_root`

This does the following:

- Installs the extension from the specified stack-product or feature-pack installation image
 - Generates the customization jobs to the location specified by `profilePath` in the response file (any existing customization jobs at this location are replaced)
 - Allocates the target CNTL and DATA datasets using the high-level qualifier specified by `targetHLQ` in the response file
 - Transfers the generated jobs from the file system to the CNTL and DATA datasets
- `zpmc.sh -workspace eclipse_workspace_dir -listExtensions`
This generates a list of the extensions that are currently installed in the specified Eclipse workspace directory.
 - `zpmc.sh -workspace eclipse_workspace_dir -uninstallExtension extension_name -version extension_version`
This removes the specified version of the specified extension from the specified Eclipse workspace directory.

Variables for using the `zpmc` command to create z/OS standalone application servers with the feature pack installed

The `zpmc` command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a standalone application server with the feature pack installed.

Action

create

Profile information

Profile name (`profileName`)

Name assigned to the generated customization jobs

Profile path (`profilePath`)

Profile path

Template path (`templatePath`)

Template path

Target dataset information

Target operating system (`targetOS`)

Target operating system

High-level qualifier (`zTargetHLQ`)

High-level qualifier for the target z/OS data sets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create

separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as "config_hlq") to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 7.0:

```
SYSPROG1.WAS70.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS70.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS70.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

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

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Volume, or '*' for SMS (zConfigHfsVolume)

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

Product file system information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasmppe.

Feature-pack file system information

Product file system directory (zScaSmpePath)

Name of the directory where feature-pack files reside after installation

Intermediate symbolic link? (zEnableScaIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Error log stream and CTRACE parmlib member information

Error log stream name (zErrorLogstreamName)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmlib member suffix (zCtraceParmlibSuffix)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Server customization

Short cell name (zCellShortName)

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a Network Deployment cell, ensure that the standalone server cell name is different from the Network Deployment cell name.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a deployment manager cell, ensure that the standalone server node name is not the same as that of any existing node in the Network Deployment cell.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Note: If this server is converted into a clustered server, this name becomes the cluster short name. The cluster short name is the WLM APPLENV name for all servers that are part of the same cluster.

Rule: Name must be eight or fewer characters and all uppercase.

JVM mode (zJvmMode)

Specify whether the JVM mode is 31 or 64 bit.

Admin asynch operations procedure name (zAdminAsynchProcName)

This specifies the JCL procedure name of a started task that is launched by way of the START command by node agents or application servers to perform certain asynchronous administrative operations (such as node synchronization) and add and remove a node.

Asynchronous administration user ID (zAdminAsynchTaskUserid)

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

Asynchronous administration UID (zAdminAsynchTaskUid)

User identifier associated with the user ID is used to run asynchronous administration operations procedure

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

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Install administrative console? (zInstallAdminConsole)

Specify whether you do (true) or do not (false) want to deploy the WebSphere Application Server for z/OS administrative console.

Note: These applications are not supported in a Network Deployment cell.

Install default application? (zInstallDefaultApp)

Specify whether you do (true) or do not (false) want to deploy the default WebSphere Application Server for z/OS application.

Install samples? (zInstallSamples)

Specify whether you do (true) or do not (false) want to deploy the WebSphere Application Server for z/OS sample applications (the Samples Gallery).

Note: These applications are not supported in a Network Deployment cell. Install the sample applications to use the application server and evaluate the latest technological advancements. The sample applications are not recommended for deployment to production application server environments.

Samples password (samplesPassword)

Password for the samples user account

Server address space information

Rule: In the following, unless specified otherwise, names must be eight or fewer characters.

Controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the application server controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the application server controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

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

Servant information

Procedure name (zServantProcName)

Name of member in your procedure library to start the application server servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the application server servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

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

Control region adjunct information

Procedure name (zAdjunctProcName)

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zAdjunctUserid)

User ID associated with application server control region adjuncts in the node

UID (zAdjunctUid)

User identifier associated with this user ID

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

Server TCP/IP information

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

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

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOP requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB port (zOrbListenerPort)

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests

Rule: Value cannot be 0.

ORB SSL port (zOrbListenerSslPort)

Port for secure IIOP requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's Web container should listen for incoming HTTP requests

The default is *, which instructs the Web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

HTTP transport port (zHttpTransportPort)

Port for HTTP requests

Rule: Value cannot be 0.

HTTPS transport port (zHttpTransportSslPort)

Port for secure HTTP requests

Rule: Value cannot be 0.

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses "local comm" communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zHighAvailManagerPort)

Port on which the High Availability Manager listens

Rule: Value cannot be 0.

Service integration port (zServiceIntegrationPort)

Port for service-integration requests

Rule: Value cannot be 0.

Service integration secure port (zServiceIntegrationSecurePort)

Port for secure service-integration requests

Rule: Value cannot be 0.

Service integration MQ interoperability port (zServiceIntegrationMqPort)

Port for service-integration MQ interoperability requests

Rule: Value cannot be 0.

Service integration MQ interoperability secure port (zServiceIntegrationSecureMqPort)

Port for secure service-integration MQ interoperability requests

Rule: Value cannot be 0.

Session initiation protocol (SIP) port (zSessionInitiationPort)

Port for session initiation requests

Rule: Value cannot be 0.

Session initiation protocol secure port (zSessionInitiationSecurePort)

Port for secure session initiation requests

Rule: Value cannot be 0.

Location service daemon customization

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

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

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

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select true to generate a new CA certificate. Select false to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select true if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify true, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to include a SAF prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID

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

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

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

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (`adminUserName`)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (`adminPassword`)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Security certificate customization should be done only if product-managed security or no security has been specified.

Default personal certificate

Issued to distinguished name (`personalCertDN`)

Identifier of the personal certificate

Issued by distinguished name (`signingCertDN`)

Identifier of the root signing certificate

Expiration period in years (`personalCertValidityPeriod`)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (`signingCertValidityPeriod`)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (`keyStorePassword`)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Web server customization

Note:

Only one Web server can be defined on a standalone application server.

Create a Web server definition (`webServerCheck`)

Web server type (`webServerType`)

Valid values: IHS, HTTPSERVER_ZOS, APACHE, IPLANET, DOMINO, IIS

Web server operating system (webServerOS)

Valid values: Windows, Linux, Solaris, AIX, HPUX, OS390, OS400

Web server name (webServerName)

Name used in defining the Web server in the administrative console

Web server host or IP address (webServerHostname)

IP name or address of the z/OS system on which the Web server is located

Web server port (webServerPort)

HTTP Port on which the Web server is listening

Web server installation directory path (webServerInstallPath)

Varies by user configuration

Web server plug-in installation directory path (webServerPluginPath)

Varies by user configuration

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for using the zpmtd command to enable existing z/OS standalone application servers for the feature pack

The zpmtd command uses the values that you specify for the variables defined in a response file to create customization data and instructions for augmenting an existing standalone application server with the feature pack.

Action

augment

Profile information**Profile name (profileName)**

Name assigned to the generated customization jobs

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information**Target operating system (targetOS)**

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS data sets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create

separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as "config_hlq") to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 7.0:

```
SYSPROG1.WAS70.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS70.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS70.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

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

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Product file system information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Feature-pack file system information

Product file system directory (zScaSmpePath)

Name of the directory where feature-pack files reside after installation

Intermediate symbolic link? (zEnableScaIntermediateSymlinkh)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security customization—z/OS-managed security**SAF profile prefix (zSAFProfilePrefix)**

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for using the zpmt command to create z/OS deployment managers with the feature pack installed

The zpmt command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a deployment manager with the feature pack installed.

Action

create

Server type

Server type (serverType)

Type of server to be created within this management profile

Profile information

Profile name (profileName)

Name assigned to the generated customization jobs

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS data sets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as "config_hlq") to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 7.0:

```
SYSPROG1.WAS70.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS70.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS70.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

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

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Volume, or '*' for SMS (zConfigHfsVolume)

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders (3390).

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

Product file system information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasmppe.

Feature-pack file system information

Product file system directory (zScaSmpePath)

Name of the directory where feature-pack files reside after installation

Intermediate symbolic link? (zEnableScaIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Error log stream and CTRACE parmlib member information

Error log stream name (zErrorLogstreamName)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmlib member suffix (zCtracedParmlibSuffix)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Server customization

Short cell name (zCellShortName)

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Note: The deployment manager is not clusterable, so this value never actually becomes the cluster short name of this server's cluster. However, like an application server, the deployment manager still needs an APPLENV, so the cluster transition name is used for this purpose.

Rule: Name must be eight or fewer characters and all uppercase.

Server address space information

Rule: In the following, unless specified otherwise, names must be eight or fewer characters.

Controller information**Procedure name (zControlProcName)**

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

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

Servant information**Procedure name (zServantProcName)**

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

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

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Server TCP/IP information

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

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

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Cell discovery address port (zCellDiscoveryPort)

Port number used by node agents to connect to this deployment manager server.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOP requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB port (zOrbListenerPort)

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests

Rule: Value cannot be 0.

ORB SSL port (zOrbListenerSslPort)

Port for secure IIOP requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's Web container should listen for incoming HTTP requests

The default is *, which instructs the Web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses "local comm" communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zHighAvailManagerPort)

Port on which the High Availability Manager listens

Rule: Value cannot be 0.

DataPower appliance manager secure inbound port (zDataPowerManagementPort)

Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location

service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

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

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select true to generate a new CA certificate. Select false to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select true if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify true, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local

OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to include a SAF prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID.

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

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

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

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (adminUserName)

Enter an alphanumeric user ID that you will use to log on to the

administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (adminPassword)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Security certificate customization should be done only if product-managed security or no security has been specified.

Default personal certificate

Issued to distinguished name (personalCertDN)

Identifier of the personal certificate

Issued by distinguished name (signingCertDN)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (signingCertValidityPeriod)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for using the zpmt command to enable existing z/OS deployment managers for the feature pack

The zpmt command uses the values that you specify for the variables defined in a response file to create customization data and instructions for augmenting an existing deployment manager with the feature pack.

Action

augment

Profile information

Profile name (profileName)

Name assigned to the generated customization jobs

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS data sets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as "config_hlq") to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 7.0:

```
SYSPROG1.WAS70.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS70.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS70.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

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

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Product file system information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Feature-pack file system information

Product file system directory (zScaSmpePath)

Name of the directory where feature-pack files reside after installation

Intermediate symbolic link? (zEnableScaIntermediateSymlinkh)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security customization—z/OS-managed security

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for using the zpmt command to create z/OS managed (custom) nodes with the feature pack installed

The zpmt command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a managed (custom) node with the feature pack installed.

Action

create

Profile information

Profile name (profileName)

Name assigned to the generated customization jobs

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS datasets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as "config_hlq") to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 7.0:

```
SYSPROG1.WAS70.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS70.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS70.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

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

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Configuration file system customization

Mount point (zConfigMountPoint)

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Volume, or '*' for SMS (zConfigHfsVolume)

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 300 cylinders (3390).

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

Product file system information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasmppe.

Feature-pack file system information

Product file system directory (zScaSmpePath)

Name of the directory where feature-pack files reside after installation

Intermediate symbolic link? (zEnableScaIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Error log stream and CTRACE parmlib member information

Error log stream name (zErrorLogstreamName)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTRACE parmlib member suffix (zCtraceParmlibSuffix)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Server customization

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Admin asynch operations procedure name (zAdminAsynchProcName)

This specifies the JCL procedure name of a started task that is launched by way of the START command by node agents or application servers to perform certain asynchronous administrative operations (such as node synchronization) and add and remove a node.

Asynchronous administration user ID (zAdminAsynchTaskUserid)

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

Asynchronous administration UID (zAdminAsynchTaskUid)

User identifier associated with the user ID is used to run asynchronous administration operations procedure

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

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Server address space information

Rule: In the following, names must be eight or fewer characters unless specified otherwise.

Controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

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

Servant information

Procedure name (zServantProcName)

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

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

Control region adjunct information

Procedure name (zAdjunctProcName)

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zAdjunctUserid)

User ID associated with application server control region adjuncts in the node

UID (zAdjunctUid)

User identifier associated with this user ID

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

Node TCP/IP information

Note: Do not choose port values already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

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

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location

service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

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

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security customization—z/OS-managed security

For this security option, you must decide whether to include a SAF prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID

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

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

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

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (`adminUserName`)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (`adminPassword`)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Federation information

Node host name or IP address (`zFederateDmaNodeHostname`)

TCP/IP node name of the deployment manager for the Network Deployment cell

Deployment manager JMX connection type (`zFederateDmaPortType`)

RMI Connect to the deployment manager using an RMI connection

SOAP Connect to the deployment manager using a SOAP connection

Deployment manager JMX port (`zFederateDmaPort`)

JMX (Java Management Extensions) SOAP (Simple Object Access Protocol) connector port that the add-node request uses to connect to the deployment manager

It provides the federation process with knowledge of which deployment manager is the target of the federation.

Deployment manager security is enabled (`zFederateDmaSecurity`)

Specify true if administrative security is enabled on the Network Deployment cell and the deployment manager.

User ID (`zFederateDmaSecurityUserID`)

User ID with full administrative privileges for the Network Deployment cell

This is the security domain administrator user ID and cannot be changed.

Password (`zFederateDmaSecurityPassword`)

Password for user ID

Node group name (`zNodeGroupName`)

Node group into which the node will be placed.

Specify `DefaultNodeGroup` if the node is in the same sysplex as the deployment manager.

ORB listener IP name (`zFederateOrbListenerHostName`)

IP address on which the server's ORB listens for incoming IIOP requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB port (zFederateOrbPortName)

Port for IIOP requests that acts as the bootstrap port for the server and also as the port through which the ORB accepts IIOP requests

Rule: Value cannot be 0.

ORB SSL port (zFederateOrbSslPortName)

Port for secure IIOP requests

The default is 0, which allows the system to choose this port.

Short node agent server name (zFederateServerShortName)

Name of the node agent server

This is the server's job name, as specified in the MVS START command JOBNAME parameter. This value identifies the server to z/OS facilities such as SAF.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long node agent server name (zFederateServerName)

Name of the node agent and the primary external identification of the node agent server

This name identifies the server as displayed through the administrative console. The node agent server long name is set to the fixed value of nodeagent.

JMX SOAP connector port (zFederateJmxSoapConnectorPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions and is invoked through scripts such as wsadmin.sh.

Rule: Value cannot be 0.

Node discovery port (zFederateNodeDiscoveryPort)

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager

Node multicast discovery port (zFederateNodeMulticastDiscoveryPort)

Defines the multicast port through which the node agent sends discovery requests to its managed servers

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port (zFederateNodeIPv6MulticastDiscoveryPort)

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers
(NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Administrative local port (zFederateAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter
(IPC_CONNECTOR_ADDRESS)

The connector uses "local comm" communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zFederateHamCommPort)

Port on which the High Availability Manager listens
(DCS_UNICAST_ADDRESS)

Launch the node agent after node federation**(zFederateNodeAgentAfterFederation)**

Specify true if you want the node agent to be started automatically after federating a node. Otherwise, specify false.

Security certificate customization

Security certificate customization should be done only if product-managed security or no security has been specified.

Default personal certificate**Issued to distinguished name (personalCertDN)**

Identifier of the personal certificate

Issued by distinguished name (signingCertDN)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate**Expiration period in years (signingCertValidityPeriod)**

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for using the zpmt command to enable existing z/OS managed (custom) nodes for the feature pack

The zpmt command uses the values that you specify for the variables defined in a response file to create customization data and instructions for augmenting an existing managed (custom) node with the feature pack.

Action

augment

Profile information**Profile name (profileName)**

Name assigned to the generated customization jobs

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information**Target operating system (targetOS)**

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS data sets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as "config_hlq") to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 7.0:

```
SYSPROG1.WAS70.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS70.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS70.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

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

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Configuration file system customization**Mount point (zConfigMountPoint)**

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Product file system information

Product file system directory (zSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Feature-pack file system information

Product file system directory (zScaSmpePath)

Name of the directory where feature-pack files reside after installation

Intermediate symbolic link? (zEnableScaIntermediateSymlinkh)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security customization—z/OS-managed security

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for using the zpmt command to create z/OS Network Deployment cells with the feature pack installed

The zpmt command uses the values that you specify for the variables defined in a response file to create customization data and instructions for configuring a Network Deployment cell with the feature pack installed.

Action

create

Profile information

Profile name (profileName)

Name assigned to the generated customization jobs

Profile path (profilePath)

Profile path

Template path (templatePath)

Template path

Target dataset information

Target operating system (targetOS)

Target operating system

High-level qualifier (zTargetHLQ)

High-level qualifier for the target z/OS data sets that will contain the generated jobs and instructions

When a customization definition is uploaded to the target z/OS system, the customization jobs and files are written to a pair of partitioned datasets. While it is possible to reuse these datasets, it is safest to create separate datasets for each WebSphere Application Server for z/OS configuration. The best practice is to use the customization dataset name prefix (sometimes referred to as "config_hlq") to indicate the version and release of WebSphere Application Server for z/OS, the task that you are performing, and the cell (as well as the node name in some cases) that you are configuring. For example, you might use the following dataset name prefix for configuring a standalone WebSphere Application Server cell named TESTCELL for Version 7.0:

```
SYSPROG1.WAS70.TESTCELL.APPSERV
```

In this example, the following two datasets will be created when the customization definition is uploaded to the target z/OS system:

```
SYSPROG1.WAS70.TESTCELL.APPSERV.CNTL  
SYSPROG1.WAS70.TESTCELL.APPSERV.DATA
```

The CNTL dataset will be a partitioned dataset (PDS) with fixed block 80-byte records that will contain the customization jobs. The DATA dataset will be a PDS with variable length data to contain the other customization data.

Rule: The high-level qualifier can consist of multiple qualifiers (up to 39 characters).

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

HLQ.CNTL

Partitioned dataset with fixed block 80-byte records to contain customization jobs

HLQ.DATA

Partitioned dataset with variable-length data to contain other data contained in the customization definition

Tip: A multilevel high-level qualifier can be specified as the dataset high-level qualifier.

Common group configuration

Configuration group (zConfigurationGroup)

Allow OS security to assign GID (zConfigurationGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zConfigurationGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zServantGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)

Specify * to allow operating-system security to assign the group ID.

Assign user-specified GID (zLocalUserGroupGID)

Specify an ID to use a specific ID.

Rule: GID values must be unique numeric values between 1 and 2,147,483,647.

System locations

System name (zSystemName)

System name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Sysplex name (zSysplexName)

Sysplex name for the target z/OS system on which you will configure WebSphere Application Server for z/OS

Tip: If you are not sure what the system name (&SYSNAME) and sysplex name (&SYSPLEX) are, use the console command D SYMBOLS on the target z/OS system to display them.

PROCLIB (zProclibName)

An existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Deployment manager configuration file system customization**Mount point (zConfigMountPoint)**

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Volume, or '*' for SMS (zConfigHfsVolume)

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders (3390).

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zFilesystemType)

This is the type of file system that will be used when creating the WebSphere for z/OS configuration file system. The default is HFS.

Application server configuration file system customization**Mount point (zAppServerConfigMountPoint)**

Read/write file system directory mount point where application data and environment files are written

The customization process creates this mount point if it does not already exist.

Name (zAppServerConfigHfsName)

File system dataset that you will create and mount at the above mount point

Rule: You can specify up to 44 characters for the dataset names.

Directory path name relative to mount point (zAppServerWasServerDir)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Volume, or '*' for SMS (zAppServerConfigHfsVolume)

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

Primary allocation in cylinders (zAppServerConfigHfsPrimaryCylinders)

Initial size allocation in cylinders for the above dataset

Recommendation: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zAppServerConfigHfsSecondaryCylinders)

Size of each secondary extent in cylinders

Recommendation: The minimum suggested size is 100 cylinders.

File system type (HFS or ZFS) (zAppServerFilesystemType)

Type of file system that will be used when creating the WebSphere for z/OS configuration file system

The default is HFS.

Deployment manager file system information**Product file system directory (zSmpePath)**

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Intermediate symbolic link? (zEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value for zEnableIntermediateSymlink is true.

Intermediate symbolic link (zIntermediateSymlink)

The default value for zIntermediateSymlink is the zConfigMountPoint value appended by /wasmppe.

Feature-pack deployment manager file system information**Product file system directory (zScaSmpePath)**

Name of the directory where feature-pack deployment manager files reside after installation

Intermediate symbolic link? (zEnableScaIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Application server file system information

Product file system directory (zAppServerSmpePath)

Name of the directory where WebSphere Application Server for z/OS files reside after installation

Intermediate symbolic link? (zAppServerEnableIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

Intermediate symbolic link (zAppServerIntermediateSymlink)

The default value for zAppServerIntermediateSymlink is the zAppServerConfigMountPoint value appended by /wasmppe.

Feature-pack application server file system information

Product file system directory (zAppServerScaSmpePath)

Name of the directory where feature-pack application server files reside after installation

Intermediate symbolic link? (zAppServerEnableScaIntermediateSymlink)

Specify true to set up an intermediate symbolic link, and specify the path name of that link if you select it.

If you specify an intermediate symbolic link, symbolic links are created from the configuration file system to the intermediate symbolic link; otherwise, they are created directly to the product file system.

The default value is true.

Intermediate symbolic link (zAppServerScaIntermediateSymlink)

The default value is the zConfigMountPoint value appended by /fpscasmpe.

Error log stream and CTRACE parmlib member information

Error log stream name (zErrorLogstreamName)

Name of the error log stream that you create

Rules:

- Name must be 26 or fewer characters.
- Do not put quotes around the name.

CTTRACE parmlib member suffix (zCtraceParmlibSuffix)

Value that is appended to CTIBBO to form the name of the CTRACE parmlib member that is used by the associated WebSphere Application Serve for z/OS daemon

The BBOCTIOO sample parmlib member in the SBBOJCL dataset can be used to create this CTRACE parmlib member.

Deployment manager server customization

Short cell name (zCellShortName)

Name that identifies the cell to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique among all other cells in the sysplex.

Long cell name (cellName)

Primary external identification of this WebSphere Application Server for z/OS cell

This name identifies the cell as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique among all other cells in the sysplex.

Short node name (zNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Long node name (nodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.
- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Short server name (zServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (serverName)

Name of the server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.

Cluster transition name (zClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Note: The deployment manager is not clusterable, so this value never actually becomes the cluster short name of this server's cluster. However, like an application server, the deployment manager still needs an APPLENV, so the cluster transition name is used for this purpose.

Rule: Name must be eight or fewer characters and all uppercase.

Application server customization

Short node name (zAppServerNodeShortName)

Name that identifies the node to z/OS facilities such as SAF

Rules:

- Name must be eight or fewer characters and all uppercase.
- Name must be unique within the cell.

Short server name (zAppServerServerShortName)

This value identifies the server to z/OS facilities such as SAF.

Note: The server short name is also used as the server JOBNAME.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long server name (zAppServerServerName)

Name of the application server and the primary external identification of this WebSphere Application Server for z/OS server

This name identifies the server as displayed through the administrative console.

Rules:

- Name must be 50 or fewer characters.
- Name can include mixed-case alphabetic characters.

Long node name (appServerNodeName)

Primary external identification of this WebSphere Application Server for z/OS node

This name identifies the node as displayed through the administrative console.

Note: If you intend to ever add this standalone server node to a deployment manager cell, ensure that the standalone server node name is not the same as that of any existing node in the Network Deployment cell.

Rules:

- Name must be 50 or fewer characters.
- Name can be of mixed case.
- Name must be unique within the cell.

- The application server must be defined on its own node; no other server can exist on the same node as the application server.

Cluster transition name (zAppServerClusterTransitionName)

WLM APPLENV (WLM application environment) name for this server

Rule: Name must be eight or fewer characters and all uppercase.

JVM mode (zJvmMode)

Specify whether the JVM mode is 31 or 64 bit.

WebSphere Application Server user ID home directory (zUserIDHomeDirectory)

New or existing file system directory in which home directories for WebSphere Application Server for z/OS user IDs will be created by the customization process

Admin asynch operations procedure name (zAdminAsynchProcName)

This specifies the JCL procedure name of a started task that is launched by way of the START command by node agents or application servers to perform certain asynchronous administrative operations (such as node synchronization) and add and remove a node.

Asynchronous administration user ID (zAdminAsynchTaskUserid)

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

Asynchronous administration UID (zAdminAsynchTaskUid)

User identifier associated with the user ID is used to run asynchronous administration operations procedure

Install administrative console? (zInstallAdminConsole)

Specify whether you do (true) or do not (false) want to deploy the WebSphere Application Server for z/OS administrative console.

Note: These applications are not supported in a Network Deployment cell.

Install default application? (zInstallDefaultApp)

Specify whether you do (true) or do not (false) want to deploy the default WebSphere Application Server for z/OS application.

Install samples? (zInstallSamples)

Specify whether you do (true) or do not (false) want to deploy the WebSphere Application Server for z/OS sample applications (the Samples Gallery).

Note: These applications are not supported in a Network Deployment cell.

Install the sample applications to use the application server and evaluate the latest technological advancements. The sample applications are not recommended for deployment to production application server environments.

Samples password (samplesPassword)

Password for the sample applications

Server address space information

Rule: In the following, names must be eight or fewer characters unless specified otherwise.

Deployment manager controller information

Procedure name (zControlProcName)

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zControlUserid)

User ID associated with the controller

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zControlUid)

User identifier associated with this user ID

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

Deployment manager servant information

Procedure name (zServantProcName)

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zServantUserid)

User ID associated with the servant

Note: If you are using a non-IBM security system, the user ID might have to match the procedure name. Please refer to your security system's documentation.

UID (zServantUid)

User identifier associated with this user ID

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

Application server controller information

Procedure name (zAppServerControlProcName)

Name of member in your procedure library to start the controller

Rule: Name must usually contain seven or fewer all-uppercase characters.

Application server servant information

Procedure name (zAppServerServantProcName)

Name of member in your procedure library to start the servant

Rule: Name must usually contain seven or fewer all-uppercase characters.

Application server controller adjunct information

Procedure name (zAppServerAdjunctProcName)

Name of the member in your procedure library that starts the control region adjunct

Rule: Name must usually contain seven or fewer all-uppercase characters.

Deployment manager TCP/IP information

Note: Do not choose port values that are already in use.

Node host name (hostName)

IP name or address of the system on which the server is configured

This value is used by other WebSphere Application Server for z/OS functions to connect to this server.

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

SOAP JMX Connector port (zSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

Cell discovery address port (zCellDiscoveryPort)

Port number used by node agents to connect to this deployment manager server.

ORB Listener IP name (zOrbListenerHostName)

IP address on which the server's ORB listens for incoming IIOP requests

The default is *, which instructs the ORB to listen on all available IP addresses.

ORB port (zOrbListenerPort)

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests

Rule: Value cannot be 0.

ORB SSL port (zOrbListenerSslPort)

Port for secure IIOP requests

The default is 0, which allows the system to choose this port.

HTTP transport IP name (zHttpTransportHostname)

IP address on which the server's Web container should listen for incoming HTTP requests

The default is *, which instructs the Web container to listen on all available IP addresses.

Note: The transport host name becomes the host name in the virtualhosts.xml file, which makes setting a specific IP address here less than ideal because, if you do so, you are restricting yourself to that IP address until you go into the administrative console and add another virtual host.

Administrative console port (zAdminConsolePort)

Port for HTTP requests to the administrative console

Administrative console secure port (zAdminConsoleSecurePort)

Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (zAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter

The connector uses "local comm" communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zHighAvailManagerPort)

Port on which the High Availability Manager listens

Rule: Value cannot be 0.

DataPower appliance manager secure inbound port (zDataPowerManagementPort)

Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager

Application server TCP/IP information

Note: Do not choose port values already in use.

SOAP JMX Connector port (zAppServerSoapPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol (SOAP_CONNECTOR_ADDRESS)

JMX is used for remote administrative functions, such as invoking scripts through wsadmin.sh.

Rule: Value cannot be 0.

ORB port (zAppServerOrbListenerPort)

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL port (zAppServerOrbListenerSslPort)

Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

HTTP transport port (zAppServerHttpTransportPort)

Port for HTTP requests (WC_defaulthost)

Rule: Value cannot be 0.

HTTPS transport port (zAppServerHttpTransportSslPort)

Port for secure HTTP requests (WC_defaulthost_secure)

Rule: Value cannot be 0.

Administrative interprocess communication port (zAppServerAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter (IPC_CONNECTOR_ADDRESS)

The connector uses "local comm" communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

**High Availability Manager communication port
(zAppServerHighAvailManagerPort)**

Port on which the High Availability Manager listens
(DCS_UNICAST_ADDRESS)

Rule: Value cannot be 0.

Service integration port (zAppServerServiceIntegrationPort)

Port for service-integration requests (SIB_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

Service integration secure port (zAppServerServiceIntegrationSecurePort)

Port for secure service-integration requests
(SIB_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

**Service integration MQ interoperability port
(zAppServerServiceIntegrationMqPort)**

Port for service-integration MQ interoperability requests
(SIB_MQ_ENDPOINT_ADDRESS)

Rule: Value cannot be 0.

**Service integration MQ interoperability secure port
(zAppServerServiceIntegrationSecureMqPort)**

Port for secure service-integration MQ interoperability requests
(SIB_MQ_ENDPOINT_SECURE_ADDRESS)

Rule: Value cannot be 0.

Session initiation protocol (SIP) port (zAppServerSessionInitiationPort)

Port for session initiation requests (SIP_DEFAULTHOST)

Rule: Value cannot be 0.

Session initiation protocol secure port (zAppServerSessionInitiationSecurePort)

Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Rule: Value cannot be 0.

Node agent TCP/IP information

ORB port (zNodeAgentOrbPortName)

Port for IIOP requests that acts as the bootstrap port for this server and also as the port through which the ORB accepts IIOP requests (BOOTSTRAP_ADDRESS and ORB_LISTENER_ADDRESS)

Rule: Value cannot be 0.

ORB SSL port (zNodeAgentOrbSslPortName)

Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

The default is 0, which allows the system to choose this port.

Short node agent server name (zNodeAgentServerShortName)

Name of the node agent server

This is the server's job name, as specified in the MVS START command JOBNAME parameter. This value identifies the server to z/OS facilities such as SAF.

Rule: Name must usually contain seven or fewer all-uppercase characters.

Long node agent server name (zNodeAgentServerName)

Name of the node agent and the primary external identification of the node agent server

This name identifies the server as displayed through the administrative console . The node agent server long name is set to the fixed value of nodeagent.

JMX SOAP connector port (zNodeAgentJmxSoapConnectorPort)

Port number for the JMX HTTP connection to this server based on the SOAP protocol

JMX is used for remote administrative functions and is invoked through scripts such as wsadmin.sh.

Rule: Value cannot be 0.

Node discovery port (zNodeAgentNodeDiscoveryPort)

Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager

Node multicast discovery port (zNodeAgentNodeMulticastDiscoveryPort)

Defines the multicast port through which the node agent sends discovery requests to its managed servers

The multicast IP address on which the discovery port is opened is defaulted by WebSphere Application Server for z/OS to 232.133.104.73. This default address can be changed using the administrative console. This is a CLASS D address. The valid IP range is from 224.0.0.0 to 239.255.255.255.

Node IPv6 multicast discovery port (zNodeAgentNodeIPv6MulticastDiscoveryPort)

Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers
(NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Administrative local port (zNodeAgentAdminLocalPort)

Port for the JMX connector that listens on the loopback adapter
(IPC_CONNECTOR_ADDRESS)

The connector uses "local comm" communications protocol, which means that the port is used only for communications that are local to the z/OS system image (or sysplex).

High Availability Manager communication port (zNodeAgentHamCommPort)

Port on which the High Availability Manager listens
(DCS_UNICAST_ADDRESS)

Location service daemon customization

The location service daemon is the initial point of client contact in WebSphere Application Server for z/OS. The server contains the CORBA-based location service agent, which places sessions in a cell. All RMI/IIOP IORs (for example, for

enterprise beans) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory (zDaemonHomePath)

Directory in which the location service daemon resides

This is set to the configuration file system mount point/Daemon and cannot be changed.

Daemon job name (zDaemonJobname)

Job name of the location service daemon, specified in the JOBNAME parameter of the MVS start command used to start the location service daemon

Caution: When configuring a new cell, be sure to choose a new daemon job name value.

Note: A server automatically starts the location service daemon if it is not already running.

Procedure name (zDaemonProcName)

Name of the member in your procedure library to start the location service daemon

Rule: Name must usually contain seven or fewer all-uppercase characters.

User ID (zDaemonUserid)

User ID associated with the location service daemon

UID (zDaemonUid)

User identifier associated with this user ID

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

IP name (zDaemonIPName)

Fully qualified IP name, registered with the Domain Name Server (DNS), that the location service daemon uses

The default is your node host name.

Note:

- In a sysplex, you should consider using a virtual IP address (VIPA) for the location service daemon IP name.
- Select the IP name for the location service daemon carefully. Once you have chosen a name, it is difficult to change, even in the middle of customization. This name must not be a numeric, such as, 3.7.2543.

Daemon listen IP (zDaemonListenIP)

The default value is *.

Rule: The default is * or a numeric IP address.

Port (zDaemonPort)

Port number on which the location service daemon listens

Note: Select the port number for the location service daemon carefully. You can choose any value you want, but, once chosen, it is difficult to change, even in the middle of customization.

SSL Port (zDaemonSSLPort)

Port number on which the location service daemon listens for SSL connections

Register daemon with WLM DNS (zDaemonRegisterWlmDns)

If you use the WLM DNS (connection optimization), you must select true to register your location service daemon with it. Otherwise, select false.

Note: Only one location service daemon per LPAR can register its domain name with WLM DNS. If you have multiple cells in the same LPAR and register one location service daemon and then a second, the second will fail to start.

SSL customization

If you plan to enable administrative security at some point, as is recommended, fill in the following SSL values:

Certificate authority keylabel (zSSLCaKeylabel)

Name of the key label that identifies the certificate authority (CA) to be used in generating server certificates

Generate certificate authority (CA) certificate (zGenerateCaCertificate)

Select true to generate a new CA certificate. Select false to have an existing CA certificate generate server certificates.

Expiration date for certificates (zCaAuthorityExpirationDate)

Expiration date used for any X509 Certificate Authority certificates as well as the expiration date for the personal certificates generated for WebSphere Application Server for z/OS servers.

You must specify this even if you selected false for Generate Certificate Authority (CA) certificate.

Default SAF key ring name (zDefaultSAFKeyringName)

Default name given to the RACF key ring used by WebSphere Application Server for z/OS

The key ring names created for repertoires are all the same within a cell.

Enable writable SAF keyring support (zEnableWritableKeyring)

Select true if you want to enable writable SAF key ring support

Enable SSL on location service daemon (zEnableSslOnDaemon)

Select true if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you specify true, a RACF key ring will be generated for the location service daemon to use.

Security customization

You can choose one of the following three options for administrative security.

Option 1: z/OS-managed security (zAdminSecurityType=websphereForZos)

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users. The EJBROLE profile will be used to control role-based access to applications. An administrator user ID and an unauthenticated user ID will be created and defined in the security database. Select this option if the WebSphere Application Server environment will run entirely on z/OS with a shared SAF-compliant (Local

OS) user registry, or if you plan to implement a non-Local OS user registry (such as LDAP) with mapping to SAF user IDs.

Option 2: Product-managed security (zAdminSecurityType=websphereFamily)

Use a simple file-based registry to define WebSphere Application Server users. An administrator user ID will be created and defined in the file-based registry.

Option 3: No security (zAdminSecurityType=none)

Do not enable administrative security. This option is not recommended.

Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Depending on the security option you choose, there may be additional values you need to set.

Security customization—z/OS-managed security

For this security option, you must decide whether to include a SAF prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

Use SAF profile prefix in RACF profiles (zSecurityDomainId)

Set this to true if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE).

SAF profile prefix (zSAFProfilePrefix)

Valid SAF profile prefix

Rule: Prefix must be eight or fewer characters.

Administrator user ID (zAdminUserid)

For Administrator user ID, enter a valid SAF user ID which will become the initial cell administrator. If this user ID already exists, it must have the WebSphere Application Server configuration group for this cell as its default UNIX System Services group.

Administrator UID (zAdminUid)

Valid UID for this user ID

Unauthenticated User ID (zAdminUnauthenticatedUserid)

Enter a valid SAF user ID which will be associated with unauthenticated client requests.

Unauthenticated UID (zAdminUnauthenticatedUid)

Valid UID for this user ID

Security customization—product-managed security

For this security option, you must choose an administrator user ID and password.

Administrator user ID (adminUserName)

Enter an alphanumeric user ID that you will use to log on to the administrative console and perform administrative tasks. This user ID and its password will initially be the only entry in the file-based user registry.

Administrator password (adminPassword)

This password must not be blank.

Security customization—no security

For this security option, there are no other choices to make. Your WebSphere Application Server environment will not be secured until you configure and enable security manually.

Security certificate customization

Security certificate customization should be done only if product-managed security or no security has been specified.

Default personal certificate

Issued to distinguished name (personalCertDN)

Identifier of the personal certificate

Issued by distinguished name (signingCertDN)

Identifier of the root signing certificate

Expiration period in years (personalCertValidityPeriod)

The default personal certificate is valid for one year. The maximum expiration is ten years.

Root signing certificate

Expiration period in years (signingCertValidityPeriod)

The default signing (root) certificate is a self-signed certificate. It has a default validation period of twenty years. The maximum validation period is twenty-five years.

Default keystore password (keyStorePassword)

The default value for the keystore password should be changed to protect the security of the keystore files and SSL configuration.

Web server customization

Create a Web server definition (webServerCheck)

Web server type (webServerType)

Valid values: IHS, HTTPSERVER_ZOS, APACHE, IPLANET, DOMINO, IIS

Web server operating system (webServerOS)

Valid values: Windows, Linux, Solaris, AIX, HPUX, OS390, OS400

Web server name (webServerName)

Name used in defining the Web server in the administrative console

Web server host or IP address (webServerHostname)

IP name or address of the z/OS system on which the Web server is located

Web server port (webServerPort)

HTTP Port on which the Web server is listening

Web server installation directory path (webServerInstallPath)

Varies by user configuration

Web server plug-in installation directory path (webServerPluginPath)

Varies by user configuration

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Applying maintenance to the Feature Pack for SCA on z/OS systems

Maintenance for the WebSphere Application Server optional materials is similar to that for the base WebSphere Application Server for z/OS product. Maintenance is applied using the System Modification Program / Extended (SMP/E), and then it is moved into production. The optional materials include feature packs and other interim deliverables.

Before you begin

Some feature-pack maintenance levels for WebSphere Application Server Version 8.0 are closely linked to specific base WebSphere Application Server maintenance levels. On distributed operating systems, feature-pack maintenance is applied automatically when base maintenance is installed. On z/OS systems, customers are responsible for upgrading feature-pack levels when this requirement is indicated in the installation materials for base service levels. Similarly, some feature pack service levels require a minimum base service level. These requirements generally are indicated in ACTION HOLD statements in the service level PTFs. If the WebSphere Application Server base service level is not appropriate for use with a specific feature-pack service level, feature-pack enabled servers do not start.

The WebSphere Application Server for z/OS service support Web site provides program temporary fix (PTF) lists for the base WebSphere Application Server for z/OS product and for each feature pack or other interim deliverable.

What to do next: Decide on the base WebSphere Application Server for z/OS maintenance level to which you will be upgrading and on which feature packs or other interim deliverables you need to upgrade.

Contact the IBM Software Support Center or consult the WebSphere Application Server for z/OS service support Web site to determine the PTFs for the required feature pack or interim deliverable maintenance levels, and order or download these PTFs.

1. Make copies of both the WebSphere Application Server for z/OS datasets (including the product file system) and the WebSphere Application Server for z/OS optional-materials datasets, including the optional-materials file systems.
2. Mount the WebSphere Application Server and optional-materials file systems at your usual service mount point. Be sure to mount the product-specific optional-materials file systems at the appropriate mount points inside the optional-materials file system.
3. Apply base WebSphere Application Server for z/OS maintenance using SMP/E.
4. Apply the required feature pack or other interim deliverable service using SMP/E.

The base product and the optional materials can be applied using either a single APPLY command in SMP/E or separate APPLY commands.

5. Unmount the WebSphere Application Server and optional-materials file systems from the service mount points, and remount them on your production systems.
6. Follow your accustomed maintenance procedures to move your WebSphere Application Server for z/OS runtime environments to the new service level.
When the post-installer runs for each node, it makes any necessary configuration file system changes for both the base WebSphere Application Server product and any feature packs enabled on the node. The applyPTF.sh command output will contain a log of all changes made.

What to do next

The WebSphere Application Server for z/OS nodes that are upgraded to the new service level are now running with compatible WebSphere Application Server for z/OS and optional-materials maintenance.

Restarting a WebSphere Application Server for z/OS node at a previous service level normally involves simply switching the runtime to use the previous level of code (datasets and product file system); the post-installer checks that any configuration changes made since the old level are backwards compatible.

New service levels that are not backwards compatible have this fact flagged in an ACTION HOLD statement for the service PTFs; customers who need to restart at the earlier service level will need to run the backoutPTF.sh command. To back out configuration changes for feature packs or other optional materials, specify the feature-pack identifier (rather than "WebSphere") in the backoutPTF.sh command:
`backoutPTF.sh SCA target_service_level`

Chapter 5. Managing profiles on non-z/OS operating systems

You can create, delete, augment, and unaugment profiles, which are sets of files that define the runtime environment. At least one profile must exist to run the product.

Before you begin

Distributed platforms This task assumes a basic familiarity with the **manageprofiles** command, the Profile Management Tool, system commands, and profile concepts.

i5/OS This task assumes a basic familiarity with the **manageprofiles** command to create additional profiles.

About this task

Typically, you create a profile when you install the product. Depending on which WebSphere Application Server product you have, you might create additional profiles.

Distributed platforms You can create profiles using the Profile Management Tool or the **manageprofiles** command.

i5/OS The Profile Management tool is unavailable. You can use the **manageprofiles** QShell script to create additional profiles. You can also use the IBM Web Administration for i5/OS[®] graphical user interface to create standalone application server profiles.

i5/OS To create an application server profile enabled for a feature pack, you must use the **manageprofiles** command.

For the Network Deployment product, you can create any combination of profiles.

Linux **HP-UX** **Solaris** **AIX** Non-root users can create their own profiles so that they can manage their own application servers. Typically, non-root users manage application servers for development purposes.

You can delete profiles through the **manageprofiles** command or by other means if necessary. You might delete a profile if the configuration that you specified in the profile is not what you want.

Perform any of the following tasks to manage profiles.

- **i5/OS** Create default profiles.
Create default profiles for WebSphere Application Server, Web servers, and application clients when you install Version 7 of the product. Default profiles are not created when you install a feature pack.
- **Distributed platforms** Create profiles using the Profile Management Tool.
- Create profiles using the **manageprofiles** command.
- **Distributed platforms** Augment profiles using the Profile Management Tool.
- Augment and unaugment profiles using the **manageprofiles** command.
- Delete profiles.

Results

You might have created, augmented, unaugmented, or deleted a profile depending on the tasks that you completed.

What to do next

Depending on the action that you completed, you can start a server or proceed to other tasks such as deploying an application.

Profile concepts

A profile defines the runtime environment. The profile includes all the files that the server processes in the runtime environment and that you can change.

Distributed platforms You can create a runtime environment either through the **manageprofiles** command or the Profile Management Tool graphical user interface. You can use the Profile Management Tool to enter most of the parameters that are described in this topic. Some parameters, however, require you to use the **manageprofiles** command. You must use the **manageprofiles** command to delete a profile, for instance, because the Profile Management Tool does not provide a deletion function. You can use either the Profile Management Tool or the **manageprofiles** command to create a cell profile. The Profile Management Tool creates the cell in a single step, whereas the **manageprofiles** command requires two separate invocations.

i5/OS You can create a runtime environment through the **manageprofiles** command. Depending on the operation that you want to perform with the **manageprofiles** command, you need to provide one or more parameters. You can use the command to do such actions as creating or deleting profiles. To create a cell profile, you must invoke the **manageprofiles** command two separate times.

Core product files

The core product files are the shared product binary files, which are shared by all profiles.

The directory structure for the product has the following two major divisions of files in the installation root directory for the product:

- The core product files are shared product binary files that do not change unless you install a refresh pack, a fix pack, or an interim fix. Some log information is also updated.

Distributed platforms The following list shows default installation locations for root users on supported platforms:

- **AIX** /usr/IBM/WebSphere/AppServer
- **Linux** **HP-UX** **Solaris** /opt/IBM/WebSphere/AppServer
- **Windows** C:\Program Files\IBM\WebSphere\AppServer

i5/OS The default installation location for the core product files is the *app_server_root* directory.

- **Distributed platforms** The *app_server_root/profiles* directory is the default directory for creating profiles.
- **i5/OS** The *app_server_root/profiles* directory is the default directory for creating profiles.

When you want binary files at different service levels, you must use a separate installation of the product for each service level.

The configuration for every defined application server process is within the profiles directory unless you specify a new directory when you create a profile. These files change as often as you create a new profile, reconfigure an existing profile, or delete a profile.

Distributed platforms Each of the folders except for the profiles directory and a few others such as the logs directory and the properties directory do not change, unless you install service fixes. The profiles directory, however, changes each time you add, change, or delete a profile. The profiles directory is the default repository for profiles. However, you can put a profile anywhere on the machine or system, provided enough disk space is available.

Distributed platforms If you create a profile in another existing folder in the installation root directory, then a risk exists that the profile might be affected by the installation of a service fix that applies maintenance to the folder. Use a directory outside of the installation root directory when using a directory other than the profiles directory for creating profiles.

i5/OS If you create a profile in an installation root directory, then a risk exists that the profile might be damaged or destroyed by routine system maintenance.

Why and when to create a profile

The **manageprofiles** command-line tool defines each profile for the product.

Distributed platforms Run the Profile Management Tool or the **manageprofiles** command each time that you want to create a profile. A need for more than one profile on a machine is common.

i5/OS Run the command-line tool each time that you want to create a profile.

Administration is greatly enhanced when using profiles instead of multiple product installations. Not only is disk space saved, but updating the product is simplified when you maintain a single set of product core files. Also, creating new profiles is more efficient and less prone to error than full product installations, allowing a developer to create separate profiles of the product for development and testing.

i5/OS You can run the **manageprofiles** command to create a new profile on the same machine as an existing profile. Define unique characteristics, such as profile name and node name, for the new profile.

Distributed platforms You can run the Profile Management Tool or the command-line tool to create a new profile on the same machine as an existing profile. Define unique characteristics, such as profile name and node name, for the new profile. Each profile shares all runtime scripts, libraries, the Java™ SE Runtime Environment 6 (JRE 6) environment, and other core product files.

Why and when to augment a profile

Additional release and service stream capabilities can require you to augment existing profiles to use the new capabilities. For instance, if you created a profile when you first installed the product and then added a feature pack that requires

changes to the profile to take advantage of the new capabilities, then you have to augment the profile. However, a feature pack might also support creating a profile that is specific to the feature pack and that already contains the capabilities needed for the feature pack. In this situation, do not complete a separate augmentation of the profile because the profile is automatically augmented when you create the profile.

Although the management profile, the cell profile, the custom profile, secure proxy profile, and the application server profile are the available profile types, a particular feature pack might support only a subset of these profile types to be created or augmented with specific feature pack capabilities.

You can create an application server profile, a cell profile, a custom profile, or a deployment manager profile that is enabled for the Feature Pack for Service Component Architecture (SCA). You also can augment Version 7 versions of these profiles to add SCA capabilities. The secure proxy profile and the management profile with a job manager server type or with an administrative agent server type do not require augmentation.

You can create a new profile with feature-pack functionality or augment an existing profile with the feature pack using the **manageprofiles** command or the Profile Management Tool.

Profile types

Templates for each profile are located in the `app_server_root/profileTemplates` directory unless they are feature pack templates.

Templates for the Feature Pack for SCA are located in the `app_server_root/profileTemplates/SCA` directory.

Multiple directories exist within this directory, which correspond to different profile types and vary with the type of product that is installed. The directories are the paths that you indicate while using the **manageprofiles** command with the `-templatePath` option. You can also specify profile templates that exist outside the `profileTemplates` directory, if you have any.

See the `-templatePath` parameter description in the **manageprofiles** command topic for more information.

The **manageprofiles** command in the Network Deployment product can create the following types of profiles:

Management profile with a deployment manager server for the Feature Pack for SCA The basic function of the deployment manager is to deploy applications to a cell of application servers, which it manages. Each application server that belongs to the cell is a *managed node*.

Distributed platforms You can create the management profile with a deployment manager server using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/management` for the `-templatePath` parameter and `DEPLOYMENT_MANAGER` for the `-serverType` parameter.

Distributed platforms If you want to create a deployment manager profile that is enabled for the Feature Pack for SCA, you can create the profile using

the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/SCA/dmgr.scafe` for the `-templatePath` parameter.

i5/OS If you want to create a deployment manager profile that is enabled for the Feature Pack for SCA, specify `SCA/dmgr.scafe` for the template parameter on the **manageprofiles** command.

Management profile with an administrative agent server

The basic function of the administrative agent is to provide a single interface to administer multiple unfederated application servers.

The management profile with an administrative agent does not require feature-pack capability. However, you can create the management profile with an administrative agent for the Network Deployment product and then use the profile in a feature-pack environment.

Distributed platforms You can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/management` for the `-templatePath` parameter and `ADMIN_AGENT` for the `-serverType` parameter to create this type of management profile.

i5/OS Specify `management` for the `-templatePath` parameter and `ADMIN_AGENT` for the `-serverType` parameter to create this type of management profile with the **manageprofiles** command.

Management profile with a job manager server

The basic function of the job manager is to provide a single console to administer multiple base servers, multiple deployment managers, and do asynchronous job submission.

The management profile with a job manager does not require feature-pack capability. However, you can create the management profile with a job manager for the Network Deployment product and then use the profile in a feature-pack environment.

Application server profile

Use the application server to make applications available to the Internet or to an intranet.

An important product feature is the ability to scale up a standalone application server profile by adding the application server node into a deployment manager cell. Multiple application server processes in a cell can deploy an application that is in demand. You can also remove an application server node from a cell to return the node to the status of a standalone application server.

Each standalone application server can optionally have its own administrative console application, which you use to manage the application server. You can also use the `wsadmin` scripting facility to perform every function that is available in the administrative console application.

No node agent process is available for a standalone application server node unless you decide to add the application server node to a deployment manager cell. Adding the application server node to a cell is known as *federation*. Federation changes the standalone application server node into a managed node. You use the administrative console of the deployment manager to manage the node. If you remove the node from

the deployment manager cell, then use the administrative console and the scripting interface of the standalone application server node to manage the process.

Distributed platforms You can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/default` for the `-templatePath` parameter to create this type of profile.

Distributed platforms If you want to create an application server profile that is enabled for the Feature Pack for SCA, you can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/SCA/default.scafep` for the `-templatePath` parameter.

i5/OS If you do not specify the `-templatePath` parameter, then an application server profile that is not enabled for the Feature Pack for SCA is created by default. You can alternatively specify `SCA/default.scafep` on the `-templatePath` parameter to create an application server profile enabled for the Feature Pack for SCA or `default` on the `-templatePath` parameter to create an application server profile that is not enabled for the Feature Pack for SCA.

Cell profile

Use the cell profile to make applications available to the Internet or to an intranet under the management of the deployment manager.

Distributed platforms Creation of a cell profile generates a deployment manager and a federated node in one iteration through the Profile Management Tool. The result is a fully functional cell on a given system.

To create a cell profile using the **manageprofiles** command, you must create two portions of the profile: the cell deployment manager portion and the cell node portion. Additionally, you can have only one cell deployment manager and one cell node associated with each other when you create a cell. The initial cell profile that you create with the **manageprofiles** command is equivalent to the cell profile you create with the Profile Management Tool. After you create the initial cell profile, you can create custom profiles or standalone profiles and federate the profiles into the deployment manager.

Distributed platforms On the **manageprofiles** command, specify `app_server_root/profileTemplates/cell/dmgr` for the `-templatePath` parameter for the deployment manager and `app_server_root/profileTemplates/cell/default` for the `-templatePath` parameter for the cell node.

Distributed platforms You can create a cell profile for the Feature Pack for SCA. On the **manageprofiles** command, specify `app_server_root/profileTemplates/SCA/cell.scafep/dmgr` for the `-templatePath` parameter for the deployment manager and `app_server_root/profileTemplates/SCA/cell.scafep/default` for the `-templatePath` parameter for the cell node.

i5/OS On the **manageprofiles** command, specify `app_server_root/profileTemplates/cell/dmgr` on the `-templatePath` parameter for the deployment manager and `app_server_root/profileTemplates/cell/default` on the `-templatePath` parameter for the cell node. You can read about the cell profile type in the article on creating a cell profile with the **manageprofiles** command.

i5/OS You can create a cell profile for the Feature Pack for SCA. On the **manageprofiles** command, specify `app_server_root/profileTemplates/SCA/cell.scafep/dmgr` on the `-templatePath` parameter for the deployment manager and `app_server_root/profileTemplates/SCA/cell.scafep/default` on the `-templatePath` parameter for the cell node. You can read about the cell profile type in the article on creating a cell profile with the **manageprofiles** command.

Distributed platforms **i5/OS** After you create the two portions that make up the cell profile, you have a deployment manager and federated node. The federated node contains an application server and the default application, which contains the snoop servlet, the HitCount application, and the HelloHTML servlet.

Custom profile

Use the custom profile which belongs to a deployment manager cell, to make applications available to the Internet or to an intranet under the management of the deployment manager.

The deployment manager converts a custom profile to a managed node by adding the node into the cell. The deployment manager also converts an application server node into a managed node when you add an application server node into a cell. When either node is added to a cell, the node becomes a managed node. The node agent process is then instantiated on the managed node. The node agent acts on behalf of the deployment manager to control application server processes on the managed node. The node agent can start or stop application servers, for example.

A deployment manager can create multiple application servers on a managed node so long as the node agent process is running. Processes on the managed node can include cluster members that the deployment manager uses to balance the workload for heavily used applications.

Use the administrative console of the deployment manager to control all of the nodes that the deployment manager manages. You can also use the `wsadmin` scripting facility of the deployment manager to control any of the managed nodes. A custom profile does not have its own administrative console or scripting interface. You cannot manage the node directly with the `wsadmin` scripting facility.

A custom profile does not include default applications or a default server like the application server profile includes. A custom profile is an empty node. Add the node to the deployment manager cell. Then, you can use the administrative interface of the deployment manager to customize the managed node by creating clusters and application servers.

Distributed platforms If you want to create a custom profile that is enabled for the Feature Pack for SCA, you can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/SCA/managed.scafep` for the `-templatePath` parameter.

i5/OS If you want to create a custom profile that is enabled for the Feature Pack for SCA, specify `SCA/managed.scafep` for the `template` parameter on the **manageprofiles** command.

Secure proxy profile

Use the secure proxy server to take requests from the Internet and forward them to application servers. The secure proxy server resides in the DMZ.

The secure proxy profile does not require feature pack capability. However, you can create the secure proxy profile for the Network Deployment product and then use the profile in a feature pack environment.

Distributed platforms You can create the profile using the Profile Management Tool or the **manageprofiles** command. If you create the profile with the **manageprofiles** command, specify `app_server_root/profileTemplates/secureproxy` for the `-templatePath` parameter to create this type of profile.

i5/OS Specify `secureproxy` for the `-templatePath` parameter on the **manageprofiles** command to create this type of profile.

Default profiles

Profiles use the concept of a default profile when more than one profile exists. The default profile is set to be the default target for scripts that do not specify a profile. You can use the `-profileName` parameter with most of the scripts to enable the scripts to act on a profile other than the default profile.

i5/OS The default installation creates a cell profile, which consists of the deployment manager portion of the profile (`dmgr`) and the default portion of the profile (`default`). This default portion of the profile is pre-federated into the cell that the deployment manager manages and contains the application server (`server1`). If you create a different type of profile during installation, then the default portion of the profile might be different.

Distributed platforms The default profile name is `<profile_type><profile_number>`:

- `<profile_type>` is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- `<profile_number>` is a sequential number that is used to create a unique profile name

Addressing a profile in a multiprofile environment: When multiple profiles exist on a machine, certain commands require that you specify the `-profileName` parameter if the profile is not the default profile. In those cases, it might be easier to use the commands that are in the `bin` directory of each profile. When you issue one of these commands within the `bin` directory of a profile, the command acts on that profile unless the `-profileName` parameter specifies a different profile.

Security policy for application server profiles

In environments where you plan to have multiple standalone application servers, the security policy of each application server profile is independent of the others. Changes to the security policy in one application server profile are not synchronized with the other profiles.

Installed file set

You decide where to install the files that define a profile.

Distributed platforms The default location is in the profiles directory in the installation root directory. You can change the location on the Profile Management Tool or in a parameter when using the command-line tool. For example, assume that you create two profiles on a Linux platform with host name devhost1. The profile directories resemble the following example if you do not relocate them:

```
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01
/opt/IBM/WebSphere/AppServer/profiles/AppSrv02
```

You can specify a different directory, such as `/opt/profiles` for the profile directory using the **manageprofiles** command. For example:

```
manageprofiles.sh
-profileName AppSrv01
-profilePath /opt/profiles
```

```
manageprofiles.sh
-profileName AppSrv02
-profilePath /opt/profiles
```

Then the profile directories resemble the directories shown in the following example:

```
/opt/profiles/AppSrv01
/opt/profiles/AppSrv02
```

i5/OS The default location is in the `user_data_root/profiles` directory. You can change the location in a parameter when using the command-line tool. For example, assume that you create two profiles with host name, devhost1.

i5/OS You can specify a different directory, such as `/home/QEJBSVR/profiles/myprofile`, using the `-profilePath` parameter of the **manageprofiles** command:

```
manageprofiles
-profileName myprofile
-profilePath /home/QEJBSVR/profiles/myprofile
```

Distributed platforms The following directories exist within a typical profile. This example assumes that the profile, AppSrv01, exists:

- `app_server_root/profiles/AppSrv01/bin`
- `app_server_root/profiles/AppSrv01/config`
- `app_server_root/profiles/AppSrv01/configuration`
- `app_server_root/profiles/AppSrv01/etc`
- `app_server_root/profiles/AppSrv01/firststeps`
- `app_server_root/profiles/AppSrv01/installableApps`
- `app_server_root/profiles/AppSrv01/installedApps`
- `app_server_root/profiles/AppSrv01/installedConnectors`
- `app_server_root/profiles/AppSrv01/installedFilters`
- `app_server_root/profiles/AppSrv01/logs`
- `app_server_root/profiles/AppSrv01/properties`
- `app_server_root/profiles/AppSrv01/samples`
- `app_server_root/profiles/AppSrv01/temp`
- `app_server_root/profiles/AppSrv01/wstemp`

i5/OS The following directories exist within a typical profile. Different profile types might include different subdirectories. This example assumes that the profile, AppSrv01, exists and was created in the default directory:

i5/OS

- `user_data_root/profiles/AppSrv01/bin`
- `user_data_root/profiles/AppSrv01/config`
- `user_data_root/profiles/AppSrv01/configuration`
- `user_data_root/profiles/AppSrv01/etc`
- `user_data_root/profiles/AppSrv01/installableApps`
- `user_data_root/profiles/AppSrv01/installedApps`
- `user_data_root/profiles/AppSrv01/installedConnectors`
- `user_data_root/profiles/AppSrv01/logs`
- `user_data_root/profiles/AppSrv01/PolicyDirector`
- `user_data_root/profiles/AppSrv01/properties`
- `user_data_root/profiles/AppSrv01/samples`
- `user_data_root/profiles/AppSrv01/temp`
- `user_data_root/profiles/AppSrv01/wstemp`

Profiles: File-system requirements

A minimum amount of space must be available in the directory where you create a profile.

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. The 40 MB of space is used for log files and temporary files.

Table 114. Space requirements.

This table shows space requirements for various profiles and server types.

| Profile or server type | Space required |
|------------------------|----------------|
| Application server | 200 MB |
| Deployment manager | 30 MB |
| Administrative agent | 30 MB |
| Job manager | 30 MB |
| Custom | 10 MB |
| Cell | 230 MB |
| Secure proxy | 5 MB |

Distributed platforms

Situations in which you could have insufficient file-system space

The Profile Management Tool and the `manageprofiles` command check that the amount of file-system space needed to create the profile is available right before profile creation begins. However, a slight chance exists that the profile creation can fail due to a lack of file-system space. This failure can occasionally occur in the following situations:

- Another user performs an action, such as copying files, that occupies file-system space at the same time that either the Profile Management Tool or the **manageprofiles** command writes to the file system.
- Another program writes to the disk at the same time that either the Profile Management Tool or the **manageprofiles** command writes to it to create a profile.
- The Profile Management Tool writes its logs and the profile that it creates to the same file system at the same time.
- The **manageprofiles** command writes its logs and the profile that it creates to the same file system at the same time.

Use the following recommendations to avoid profile creation failure:

- Ensure that enough temporary space is allocated for profile creation. Some temporary space is needed for the profile creation logs. These logs can be on a different file system than the file system on which the profile is created.
- Ensure no other program writes to the file-system space when either the Profile Management Tool or the **manageprofiles** command creates the profile.
- Ensure no user performs actions that occupy the file-system space when either the Profile Management Tool or the **manageprofiles** command creates the profile.

i5/OS

Situations in which you could have insufficient file-system space

The **manageprofiles** command checks that the amount of file-system space needed to create the profile is available right before profile creation begins. However, a slight chance exists that the profile creation can fail due to a lack of file-system space. This failure can occasionally occur in the following situations:

- Another user performs an action, such as copying files, that occupies file-system space at the same time that the **manageprofiles** command writes to the file system.
- Another program writes to the disk at the same time that the **manageprofiles** command writes to it to create a profile.
- The **manageprofiles** command writes its logs and the profile that it creates to the same file system at the same time.

Use the following recommendations to avoid profile creation failure:

- Ensure that enough temporary space is allocated for profile creation. Some temporary space is needed for the profile creation logs. These logs can be on a different file system than the file system on which the profile is created.
- Ensure no other program writes to the file-system space when the **manageprofiles** command creates the profile.
- Ensure no user performs actions that occupy the file-system space when the **manageprofiles** command creates the profile.

Distributed platforms

Differences between the manageprofiles command and the Profile Management tool when creating cell profiles

Both the **manageprofiles** command and the Profile Management tool can create a cell profile that has both a federated application server profile and a deployment manager profile. However, the Profile Management tool and the **manageprofiles** command create cell profiles differently. The differences are important to

understand in terms of the available file-system space needed to create the cell profiles. You can create a cell profile in one pass through the Profile Management tool. In this case, you need 230 MB of available file-system space to create the cell profile. However, to create a cell profile using the `manageprofiles` command that is equivalent to the cell profile that the Profile Management tool creates, you must create two individual profiles, the cell deployment manager profile and the cell node profile. The cell deployment manager profile requires 30 MB of available file-system space, while the cell node profile requires 200 MB of available file-system space.

Augmentation rules and limitations for feature packs on non-z/OS operating systems

Rules and limitations apply to augmentation and unaugmentation of deployment manager, application server, custom, and cell profiles, and to interactions between nodes or nodes and the deployment manager. Use these rules and limitations to ensure a properly functioning feature-pack environment.

Augmentation rules and limitations

- The latest feature pack that you apply might require augmentation of the Network Deployment profiles or the profile of a prerequisite feature pack. If so, you can have a mix of augmented and unaugmented profiles. However, you must have at least one profile augmented for this latest feature pack to use its capabilities.
- For multiple feature packs, you must first install all the feature packs, augment the profile for each of the feature packs, and then make configuration changes for those feature packs. The order of installing or augmenting the feature packs does not matter unless a particular feature pack requires you to install another feature pack first. You can only make configuration changes after you augment the profile.
- If you have multiple feature packs installed, uninstalling one feature pack unaugments the deployment manager profile for that feature pack. The other feature packs remain usable for the deployment manager profile.
- If you have multiple feature packs installed, uninstalling one feature pack unaugments the profiles that were augmented for that feature pack. The profiles augmented for other feature packs remain augmented.

You can determine the template that was used for creating the profile by viewing the profile registry in the `profileRegistry.xml` file. By default, this file is located in the following directory:

Linux **HP-UX** **Solaris** **AIX**
`app_server_root/properties/`

Windows
`app_server_root\properties\`

gotcha: When you create the application server profile, a default `server1` process is created. If you delete the `server1` process, the profile becomes a custom profile and is governed by the rules for a custom profile.

Table 115. Rules for profile augmentation.

This table lists the augmentation rules and limitations for feature packs on non-z/OS operating systems.

| Profiles | Supported | Not supported |
|--------------------|---|---------------|
| Application server | <ul style="list-style-type: none"> • Creation of a new application server profile that is enabled for the feature pack. You must install the feature pack onto the product first. When you create the application server profile for the feature pack, the feature pack automatically augments the profile with feature-pack capabilities. • User-initiated augmentation of an application server profile. The application server profile might have had configuration changes made to it. The application server profile might have been created before or after you applied the feature pack. | |
| Deployment manager | <ul style="list-style-type: none"> • Creation of a new deployment manager profile that is enabled for the feature pack. You must install the feature pack onto the product first. When you create the deployment manager profile for the feature pack, the feature pack automatically augments the profile with feature-pack capabilities. • User-initiated augmentation of a Network Deployment management profile with a deployment manager. The configuration of the Network Deployment management profile with a deployment manager might have changed. The Network Deployment management profile with a deployment manager might have been created before or after you applied the feature pack. | |
| Custom | <ul style="list-style-type: none"> • Creation of a new custom profile that is enabled for the feature pack. You must install the feature pack onto the product first. When you create the custom profile for the feature pack, the feature pack automatically augments the profile with feature-pack capabilities. • Augmentation of a Network Deployment custom profile to enable it for a feature pack | |

Table 115. Rules for profile augmentation (continued).

This table lists the augmentation rules and limitations for feature packs on non-z/OS operating systems.

| Profiles | Supported | Not supported |
|---|---|--|
| Cell | <ul style="list-style-type: none"> Creation of a new deployment manager profile and a federated application server profile that are enabled for the feature pack. You must install the feature pack onto the Network Deployment product first. When you create the deployment manager profile and the federated application server profile for the feature pack, the feature pack automatically augments the profile with feature-pack capabilities. Augmentation of a Network Deployment cell profile to enable it for a feature pack. You must augment a deployment manager profile and create an application server profile enabled for the feature pack based on the preceding rules in this table. | |
| Management profile with an administrative agent | | Augmentation of the profile to enable it for a feature pack, as the profile has no requirements for feature-pack capability. However, you can use the profile in a feature-pack environment. |
| Management profile with a job manager | | Augmentation of the profile to enable it for a feature pack, as the profile has no requirements for feature-pack capability. However, you can use the profile in a feature-pack environment. |
| Secure proxy | | Augmentation of the profile to enable it for a feature pack, as the profile has no requirements for feature-pack capability. However, you can use the profile in a feature-pack environment. |
| Secure proxy administrative agent | | Augmentation of the profile to enable it for a feature pack, as the profile has no requirements for feature-pack capability. However, you can use the profile in a feature-pack environment. |

Unaugmentation rules and limitations

If a profile is augmented, then both the feature-pack uninstaller program and the delete profile action invoke unaugmentation actions for that profile before invoking the uninstall action or the delete action, respectively.

Whenever unaugmentation of a feature-pack profile occurs, a message is generated indicating that the applications in the profile are expected to fail.

When a deployment manager profile is unaugmented for a feature pack, other profiles augmented with the same feature pack in the cell fail.

Augmentation rules and limitations for a mixed-cell environment

When you perform tasks between nodes, or between nodes and the deployment manager, the feature packs must be compatible.

Table 116. Augmentation in a mixed-cell environment.

This table lists the augmentation rules and limitations for a mixed-cell environment.

| Function | Rules |
|---|---|
| Addition of a node | <ul style="list-style-type: none">You can add a node to a cell as long as the deployment manager has been augmented with at least the same set of feature packs as the node. The deployment manager might have been augmented with additional feature packs.You can add a node with no feature-pack profile to a cell even though the deployment manager is augmented with some feature packs.You cannot add a node with a particular feature-pack profile to a cell if the deployment manager has not been augmented with that feature pack. |
| Application installation | <ul style="list-style-type: none">You can target an application that requires feature-pack functionality to an application server on a node that has been augmented with feature packs that contain that functionality.You can target an application that does not require feature-pack functionality to an application server on a node with or without feature-pack augmentation.You cannot target an application that requires feature-pack functionality to an application server on a node that has not been augmented with that feature-pack functionality. |
| Server configuration template | <ul style="list-style-type: none">You can use the server configuration template to create a server on another node that is augmented with the same feature pack.If you attempt to use a server configuration template to create a server on another node that is augmented with a different feature pack, then the operation fails. The scenario is not supported. |
| Cluster management | <ul style="list-style-type: none">When you add a new member to a cluster, the new member must be able to run all the applications that have been targeted for the cluster.If an application targeted for the cluster requires a specific feature pack, you must add the new member from a node that is enabled with that feature pack. Otherwise, an error occurs.If no application on the cluster requires a specific feature pack, you can add the new member to the cluster from a node with a feature pack or a node without a feature pack. |
| Configuration archive export and import | <ul style="list-style-type: none">If a configuration contains feature-pack capabilities, exporting a configuration to a configuration archive and importing a configuration from a configuration archive are unsupported. The export or import might succeed in one case and fail in another case. If you run one of the export or import commands of the ConfigArchiveOperations command group against one of these configurations, the command might complete without reporting an error. No message is displayed when importing or exporting; however, do not expect the imported configuration to function correctly. |

Managing profiles using commands

Use commands to create a profile, start the server of the profile, display ports used by your server, and open the administrative console.

Before you begin

This task assumes a basic familiarity with the command, other application server commands, and system commands.

Before you can create and use a profile, you must install the product.

About this task

Perform the following steps to create a profile, start the server of the profile, display ports used by your server, and open the administrative console for your server.

Distributed platforms This example deals with the profile environment of a standalone application server.

1. Create the server profile from the original installation:

- **Windows** `app_server_root\bin\manageprofiles.bat`
- **Linux** **HP-UX** **Solaris** **AIX** `app_server_root/bin/manageprofiles.sh`
- **i5/OS** `app_server_root/bin/manageprofiles`

Assume that you create the profile by using the defaults. The following script is an example for creating an application server profile:

- **Windows** `app_server_root\bin\manageprofiles.bat -create -templatePath app_server_root\profileTemplates\default`
- **Linux** **HP-UX** **Solaris** **AIX** `app_server_root/bin/manageprofiles.sh -create -templatePath app_server_root/profileTemplates/default`
- **i5/OS** `app_server_root/bin/manageprofiles.sh -create -templatePath app_server_root/profileTemplates/default`

The following script is an example for creating an application server profile that is enabled for the Feature Pack for SCA:

- **Windows** `app_server_root\bin\manageprofiles.bat -create -templatePath app_server_root\profileTemplates\SCA\default.scafeop`
- **Linux** **HP-UX** **Solaris** **AIX** `app_server_root/bin/manageprofiles.sh -create -templatePath app_server_root/profileTemplates/SCA/default.scafeop`

2. Change directories to the `profile_root/bin` directory of the new server profile.
3. Start the server.

Issue the `startServer` command.

Windows
`startServer.bat server1 -profileName profile_name`

Linux **HP-UX** **Solaris** **AIX**
`startServer.sh server1 -profileName profile_name`

i5/OS The server name is the same name as the profile, which, in this case, is `profile_name`.

`startServer -profileName profile_name`

Note: The `-profileName` argument is not necessary if you have already changed to the `profile_root/bin` directory of the target profile.

4. Display the ports.

These are the ports assigned during profile creation.

Windows Open the portdef.props file in the *profile_root*\properties directory.

Linux **HP-UX** **Solaris** **AIX** Open the portdef.props file in the *profile_root*/properties directory.

i5/OS Use the dspwasinst QShell script to display the ports for your new profile:

```
app_server_root/bin/dspwasinst -profileName profileName
```

The WC_adminhost and WC_adminhost_secure ports listed are the nonsecure and secure administrative console ports, respectively.

5. Open the administrative console.

The server1 administrative console is defined on the WC_adminhost setting for the non-secure administrative console port or the WC_adminhost_secure setting for the secure administrative console port.

If the value of the WC_adminhost port for your server is 20003, for example, specify the following Web address in your browser:

```
http://host_name_or_IP_address:20003/ibm/console/
```

If the value of the WC_adminhost_secure port for your server is 9061, for example, specify the following Web address in your browser:

```
https://host_name_or_IP_address:9061/ibm/console/
```

Results

You created an application server profile, augmented the profile with the feature pack, started an application server, and accessed the administrative console using your browser.

What to do next

Deploy an application.

Creating profiles enabled for a feature pack using the command prompt

A profile includes all of the files that the server processes can change in the runtime environment. You can create a profile enabled for a feature pack by specifying a feature-pack profile template when you run the manageprofiles command.

Before you begin

Install the feature pack on top of an existing Network Deployment installation.

About this task

This example explains how to use the **manageprofiles** command-line tool to create application server and deployment manager runtime environments that uses the feature-pack profile templates.

Attention: Do not manually modify the files that are located in the *app_server_root/profileTemplates/SCA* directory or its subdirectories. For example, if you are changing the ports during profile creation, then use the Profile Management Tool or the **-startingPort** or **-portsFile** arguments on the **manageprofiles** command instead of modifying the file in the profile template directory.

Use the following steps to create a new profile for the feature-pack environment. This example is for a deployment manager profile.

1. Open your command utility.
 - **Distributed platforms** Open a command prompt and navigate to the `app_server_root/bin` directory.
 - **i5/OS** Start a Qshell session using the STRQSH CL command.
2. Create a deployment manager profile that uses the feature-pack environment. Be sure to specify the fully qualified file path for the `-templatePath` parameter. If a relative file path is specified for the `-templatePath` parameter, then your profile might not be fully enabled. For example, enter the following command to create a deployment manager profile enabled for the feature pack:

Windows

```
manageprofiles.bat -create -profileName Dmgr01 -templatePath  
app_server_root\profileTemplates\SCA\dmgr.scafep
```

Linux

Solaris

HP-UX

AIX

```
manageprofiles.sh -create -profileName Dmgr01 -templatePath  
app_server_root/profileTemplates/SCA/dmgr.scafep
```

i5/OS

```
manageprofiles -create -profileName Dmgr01 -templatePath  
app_server_root/profileTemplates/SCA/dmgr.scafep
```

Results

The command returns a message indicating success if a profile is created.

Augmenting a profile using the command prompt

After completing the installation of a feature pack, a feature pack might require you to augment a profile to make the profile compatible with a particular feature pack. You can augment the profile using the **manageprofiles** command.

Before you begin

Install the feature pack on an existing Network Deployment installation. For installation instructions, use the topics for installing the feature pack.

Each profile has one log file for augmentation. The augmentation log, if it exists, is overwritten if you augment the profile more than once. Optionally save the contents of the augmentation log before you start the next augmentation. You can choose the method of saving the log, such as renaming or copying the file. The augmentation log is located at:

- **Linux** **HP-UX** **Solaris** **AIX** **i5/OS** `app_server_root/logs/`
`manageprofiles/xxx_augment.log`
- **Windows** `app_server_root\logs\manageprofiles\xxx_augment.log`

`xxx` is the profile name.

About this task

This article explains how to use the **manageprofiles** command-line tool to augment a profile.

For the feature pack, you can augment the application server profile, the management profile with a server type of deployment manager, the custom profile, and the cell profile of the Network Deployment product. You cannot augment the management profile with a server type of administrative agent, the management profile with a server type of job manager, or the secure proxy profile. Read about profile augmentation rules and limitations for feature packs for additional information.

The following guidelines apply for augmenting existing profiles in a mixed-cell environment.

- You can add nodes that are configured for the feature pack to a cell if the deployment manager is augmented with the same feature-pack environment.
- You can add nodes that are not configured for the feature pack to a cell if the deployment manager is augmented with the feature-pack environment.
- You cannot add nodes that are configured for the feature pack to a cell if the deployment manager is not augmented with the feature-pack environment.

The feature pack provides profile templates during installation. These templates are located in the `app_server_root/profileTemplates/SCA` directory.

See “Profile concepts” on page 140 for detailed information about these templates and how they are used.

Do not manually modify the files that are located in the `profileTemplates` directory. For example, if you are changing the ports during profile creation, use the `-startingPort` or `-portsFile` arguments to the **manageprofiles** command instead of modifying the file in the profile template directory.

Use the following steps to augment your existing profiles that adhere to the previous guidelines. This example augments a deployment manager profile.

1. Open your command utility.

- **Distributed platforms** Open a command prompt, and navigate to the `app_server_root/bin` directory.
- **i5/OS** Start a Qshell session using the `STRQSH CL` command.

2. Back up your current deployment manager profile.

Profile augmentation might result in changes to the configuration of the profile. Use the `backupConfig` command to back up your current configuration before augmenting your profile. For example, the following command saves your current configuration to the `featurePackAugment.zip` file:

```
backupConfig(.bat)(.sh) featurePackAugment.zip
```

3. Augment your deployment manager profile for the feature-pack environment.

Use the **manageprofiles** command, specifying the fully qualified file path for the `-templatePath` parameter.

Note: **Distributed platforms** If a relative file path is specified for the `-templatePath` parameter, then your profile might not be fully augmented.

The following command example augments the `myDMGR` deployment manager profile in a Network Deployment environment:

```
Windows  
manageprofiles.bat -augment -profileName myDMGR -templatePath  
app_server_root\profileTemplates\SCA\dmgr.scafe
```

Linux **Solaris** **HP-UX** **AIX**

```
manageprofiles(.sh) -augment -profileName myDMGR -templatePath
app_server_root/profileTemplates/SCA/dmgr.scafe
```

i5/OS

```
manageprofiles -augment -profileName myDMGR -templatePath
app_server_root/profileTemplates/SCA/dmgr.scafe
```

Results

The command returns a success or failure message. If you receive the message, There are no augmenting templates available for the selected type of profile, the profile you selected cannot be augmented with the feature-pack template.

Unaugmenting a profile using the command prompt

You must unaugment or delete your profiles from your environment to remove feature-pack functionality. Use the manageprofiles command to unaugment existing profiles in a feature-pack environment.

Before you begin

Install the feature pack on top of an existing Network Deployment installation.

Remove all installed applications that require feature-pack functions that are located in the profile being unaugmented. If you unaugment profiles without removing the applications, the applications might not be usable.

About this task

There are two ways to unaugment profiles that are using a feature-pack environment:

- Uninstall the feature pack from your environment. The augmented profiles are automatically unaugmented before the uninstallation begins.
- Use the -unaugment parameter with the manageprofiles command line tool to unaugment a profile.

Complete this task to unaugment specific profiles that are augmented for the feature-pack environment using the manageprofiles command-line tool. You can unaugment a deployment manager profile, application server profile, custom profile, or cell profile that you previously augmented.

The following example unaugments an application server profile that was previously augmented for the feature pack.

1. Open your command utility.
 - **Distributed platforms** Open a command prompt, and navigate to the `app_server_root/bin` directory.
 - **i5/OS** Start a Qshell session using the STRQSH CL command.
2. Unaugment an application server profile.

Use the manageprofiles command-line tool and the -unaugment parameter to remove the configuration for the augmented feature from the profile.

The following command example unaugments a deployment manager profile that was previously augmented with the feature-pack template in a Network Deployment environment:

Windows

```
manageprofiles.bat -unaugment -profileName myDMGR -templatePath
app_server_root\profileTemplates\SCA\dmgr.scafef
```

Linux

Solaris

HP-UX

AIX

```
manageprofiles(.sh) -unaugment -profileName myDMGR -templatePath
app_server_root/profileTemplates/SCA/dmgr.scafef
```

i5/OS

```
manageprofiles -unaugment -profileName myDMGR -templatePath
app_server_root/profileTemplates/SCA/dmgr.scafef
```

Note: The `-unaugment` argument unaugments only the last augmentation applied to the profile unless both the `-templatePath` and `-ignoreStack` parameters are specified as well.

Results

The command returns a message indicating whether the profile was unaugmented successfully.

Managing profiles using the graphical user interface

You can create profiles, which define runtime environments, using the Profile Management Tool. Using profiles instead of multiple product installations saves disk space and simplifies updating the product because a single set of core product files is maintained.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Distributed platforms

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

About this task

You can have the installation procedure create a default profile. After installing the core product files for the Network Deployment product, use the Profile Management Tool or the `manageprofiles` command to create additional profiles.

- Create a cell profile.

With a cell profile, you can create a deployment manager profile and a profile for a federated application server node in a single pass through the Profile Management tool. Use the cell profile creation option to create the deployment manager profile and the federated application server node profile, unless you have a specific reason to create them separately.

After you install the Network Deployment product and apply the feature pack, you can create two different types of cell profiles: one that is enabled for the Network Deployment product only or one that is also enabled for the feature pack.

- Create a management profile with a deployment manager server.
With a deployment manager you can create the administrative node for a multinode, multi-machine group of application server nodes that you create later. This logical group of application server processes is known as a *cell*.
After you install the Network Deployment product and apply the feature pack, you can create a management profile with a deployment manager that is enabled for the Network Deployment product only or a deployment manager profile that is enabled for the feature pack.
- Create a management profile with an administrative agent server.
You can create a management profile for the administrative agent to administer multiple application servers that run customer applications only. The administrative agent provides a single administrative console to administer the application servers.
- Create a management profile with a job manager server.
You can create a management profile for the job manager to coordinate administrative actions among multiple deployment managers, administer multiple unfederated application servers, asynchronously submit jobs to start servers, and a variety of other tasks.
- Create an application server profile.
Create an application server profile so that you can make applications available to the Internet or to an intranet, typically using Java technology.
After you install the Network Deployment product and apply the feature pack, you can create two different types of application server profiles: one that is enabled for the Network Deployment product only or one that is also enabled for the feature pack.
- Create a custom profile.
A custom profile is an empty node that you can customize through the deployment manager to include application servers, clusters, or other Java processes, such as a messaging server. Create a custom profile on a distributed machine and add the node into the deployment manager cell to get started customizing the node.
After you install the Network Deployment product and apply the feature pack, you can create two different types of custom profiles: one that is enabled for the Network Deployment product only or one that is also enabled for the feature pack.
- Create a secure proxy profile.
You can create a secure proxy profile to serve as the initial point of entry into your enterprise environment. Typically, a secure proxy server exists in the DMZ, accepts requests from clients on the Internet, and forwards the requests to servers in your enterprise environment.

Results

You have created one or more profiles using the Profile Management Tool.

What to do next

See the description of the **manageprofiles** command to learn more about the command-line alternative method of creating a profile and to see examples of using the command.

Read about planning for installation for examples of configurations that you can create by creating profiles.

Creating management profiles with deployment managers

You can create a management profile for the deployment manager to administer servers within the deployment manager cell. Use the Profile Management Tool to create the profile.


Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention:  When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root/.Xdefaults* file:

```
Eclipse*spacing:0  
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the Network Deployment product, you must create a profile. This procedure describes creating a management profile with a deployment manager using the graphical user interface that is provided by the Profile Management Tool. You can also use the **manageprofiles** command to create a management profile with a deployment manager. See the description of the **manageprofiles** command for more information.

If you additionally install the feature pack, you can use either the Profile Management Tool or the manageprofiles to create a deployment manager profile for the feature pack.

The deployment manager provides a single administrative interface for a logical group of application servers on one or more machines.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

1. Start the Profile Management Tool to create a new runtime environment.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

- **Linux** **HP-UX** **Solaris** **AIX** `app_server_root/bin/ProfileManagement`
- **Windows** `app_server_root\bin\ProfileManagement`

The name of the command varies per platform:

- **Linux** **HP-UX** **Solaris** **AIX** `pmt.sh`
- **Windows** `pmt.bat`

- Select the Profile Management Tool option from the First steps console.
 - **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.
 - **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click *the_operating_system_menus_to_access_programs* > **IBM WebSphere > your_product > Profile Management Tool**.
2. Click **Create** to create a new profile.
 3. Click **Launch Profile Management Tool**, and then click **Create** on the Profiles tab to create a new profile.

The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

The tool displays the Environment selection panel.

4. Select the type of deployment manager profile that you want to create, and click **Next**.

The Server type selection panel is displayed.

- If you want to create a management profile with a deployment manager that is not enabled for the feature pack:
 - a. Select **Management** and then click **Next**.
 - b. Select **Deployment manager** and then click **Next**.
- Select **Deployment manager with Feature Pack for SCA** if you want to create a deployment manager profile that is enabled for the feature pack and then click **Next**.

5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.

6. If you selected **Typical profile creation**, go to the step on administrative security.

7. If you selected **Advanced profile creation**, optionally select to deploy the administrative console, then click **Next**.

The wizard displays the Profile name and location panel.

8. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

Profile naming guidelines: 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 * & ?
- Slashes (/) or (\)

The 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 only one profile exists on a machine, every command works on the single server process in the configuration. 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.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the `-profileName` parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

Default profile information

The default profile name is `<profile_type><profile_number>`:

- `<profile_type>` is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- `<profile_number>` is a sequential number that is used to create a unique profile name

AIX **HP-UX** **Linux** **Solaris** The default profile directory is `app_server_root/profiles`, where `app_server_root` is the installation root.

Windows The default profile directory is `app_server_root\profiles`, where `app_server_root` is the installation root.

9. On the Node, host, and cell names panel, specify a unique node name, the actual host name of the machine, and a unique cell name. Click **Next**.

Table 117. Characteristics of the deployment manager node.

This table shows the characteristics of the deployment manager node.

| Field Name | Default Value | Constraints | Description |
|------------|--|---|--|
| Node name | <i>shortHostName</i> CellManager <i>NodeNumber</i> where: <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>NodeNumber</i> is a sequential number starting at 01. | Use a unique name for the deployment manager. | The name is used for administration within the deployment manager cell. |
| Host name | The long form of the domain name server (DNS) name. | The host name must be addressable through your network. Read about Host name considerations. | Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table. |
| Cell name | <i>shortHostName</i> Cell <i>CellNumber</i> where: <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>CellNumber</i> is a sequential number starting at 01. | Use a unique name for the deployment manager cell. If you plan to migrate a Version 5 deployment manager cell or a Version 6 deployment manager cell to this Version 7, use the same cell name as the Version 5 or Version 6. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a <code>javax.naming.NameNotFoundException</code> error, in which case, create uniquely named cells. | All federated nodes become members of the deployment manager cell, which you name in this panel. |

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path considerations

Windows The number of characters in the `profiles_directory_path\profile_name` directory must be less than or equal to 80 characters.

Host name considerations

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the `hostName` property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the `hostName` property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying deployment manager characteristics, the wizard displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.
12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports within the deployment manager profile are unique, or intentionally conflicting, and click **Next**.

If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

Port conflict resolution

Ports are recognized as being in use if one of the following conditions exists:

- The ports are assigned to a profile created from an installation that is performed by the current user.
- The port is currently in use.

Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- **Linux** **HP-UX** **Solaris** **AIX** `profile_root/properties/portdef.props` file
- **Windows** `profile_root\properties\portdef.props` file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

Windows **Linux** The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the dmgr process as a Windows service on a Windows platform or as a Linux Service on a Linux platform, and click **Next**.

The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

Windows The product attempts to start Windows services for dmgr processes that are started by a **startManager** command. For example, if you configure a deployment manager as a Windows service and issue the **startManager** command, then the **wasservice** command attempts to start the defined service.

If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have Log on as a service authority for the service to run correctly. If the user does not have Log on as a service authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of Log on as a service. The Installation wizard grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the wasservice command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as *Local System*. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a *Local System* variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as *Local System*. When the Windows service for the dmgr process tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the dmgr process runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as *Local System*.

Default Windows service information

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is automatic. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than automatic, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The wizard displays the Profile Creation Summary panel.

16. Click **Create** to create the deployment manager, or click **Back** to change the characteristics of the deployment manager.

The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

When the profile creation completes, the tool displays the Profile creation complete panel.

17. Optionally, select **Launch the First steps console**. Click **Finish** to exit.
With the First steps console, you can create additional profiles and start the application server.

Results

You created a deployment manager profile.

Refer to the description of the **manageprofiles** command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Create an application server profile or a custom profile, and add the node into the cell.

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

Creating management profiles with administrative agents

You can create a management profile for the administrative agent to administer multiple application servers that run customer applications only. The administrative agent provides a single administrative console to administer the application servers.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: **Solaris** When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the `app_server_root/.Xdefaults` file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*--10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the product, you must create a profile. This procedure describes creating a management profile with an administrative agent server using the graphical user interface that is provided by the Profile Management Tool. You can also use the **manageprofiles** command to create an administrative agent. See the description of the `manageprofiles` command for more information.

You cannot create a management profile with an administrative agent that is enabled for the feature pack, as the profile has no requirements for feature-pack capability. However, you can use the profile in a feature-pack environment.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

1. Start the Profile Management Tool to create a new runtime environment.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

```
- Linux HP-UX Solaris AIX app_server_root/bin/
  ProfileManagement
- Windows app_server_root\bin\ProfileManagement
```

The name of the command varies per platform:

```
- Linux HP-UX Solaris AIX pmt.sh
- Windows pmt.bat
```

- Select the Profile Management Tool option from the First steps console.
 - **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.
 - **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click **the_operating_system_menus_to_access_programs > IBM WebSphere > your_product > Profile Management Tool**.
2. Click **Launch Profile Management Tool**, and then click **Create** on the Profiles tab to create a new profile.

The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

The tool displays the Environment selection panel.

3. Select **Management**, and click **Next**.

The Server type selection panel is displayed.

4. Select **Administrative agent**. Click **Next**.

The Profile creation options panel is displayed.

5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.

6. If you selected **Typical profile creation**, go to the step on administrative security.

7. If you selected **Advanced profile creation**, optionally select to deploy the administrative console and then click **Next**.

If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

The tool displays the Profile name and location panel.

8. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

Profile naming guidelines: 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 * & ?
- Slashes (/) or (\)

The 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 only one profile exists on a machine, every command works on the single server process in the configuration. 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.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the `-profileName` parameter to identify which profile to address. You might find it easier to use the commands that are in the bin directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

Default profile information

The default profile name is `<profile_type><profile_number>`:

- *<profile_type>* is a value of AppSrv, Dmgr, Custom, AdminAgent, JobMgr, or SecureProxySrv.
- *<profile_number>* is a sequential number that is used to create a unique profile name

AIX **HP-UX** **Linux** **Solaris** The default profile directory is *app_server_root/profiles*, where *app_server_root* is the installation root.

Windows The default profile directory is *app_server_root\profiles*, where *app_server_root* is the installation root.

9. On the Node, host, and cell names panel, specify a unique node name, the actual host name of the machine, and a unique cell name. Click **Next**.

Table 118. Characteristics of the administrative agent node.

This table shows the characteristics of the administrative agent node.

| Field name | Default value | Constraints | Description |
|------------|--|---|--|
| Node name | <i>shortHostName</i> <i>AANode</i> <i>NodeNumber</i> where: <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>NodeNumber</i> is a sequential number starting at 01. | Use a unique name for the administrative agent. | The name is used for administration within the administrative agent cell. |
| Host name | The long form of the domain name server (DNS) name. | The host name must be addressable through your network. Read about Host name considerations. | Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table. |
| Cell name | <i>shortHostName</i> <i>Cell</i> <i>CellNumber</i> where: <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>CellNumber</i> is a sequential number starting at 01. | Use a unique name for the cell. If you plan to migrate a Version 5 or Version 6 cell to Version 7, use the same cell name as the Version 5 or Version 7 cell. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a <code>javax.naming.NameNotFoundException</code> error, in which case, create uniquely named cells. | All federated nodes become members of the cell, which you name in this panel. |

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path length

Windows The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Host name considerations

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, *localhost*, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the *hostName* property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as *xmachine.manhattan.ibm.com*
- The default short DNS host name string, such as *xmachine*
- Numeric IP address, such as *127.1.255.3*

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, *127.0.0.1*, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the *hostName* property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if

you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying characteristics, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.
12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports within the administrative agent profile are unique, or intentionally conflicting, and click **Next**.

If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

Port conflict resolution

Ports are recognized as being in use if one of the following conditions exists:

- The ports are assigned to a profile created from an installation that is performed by the current user.
- The port is currently in use.

Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- **Linux** **HP-UX** **Solaris** **AIX** `profile_root/properties/portdef.props` file
- **Windows** `profile_root\properties\portdef.props` file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

Windows **Linux** The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the administrative agent process as a Windows service on a Windows operating system or as a Linux service on a Linux operating system, and click **Next**.

The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the WASService.exe command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

Windows The product attempts to start Windows services for administrative agent processes that are started by a startServer command. For example, if you configure an administrative agent as a Windows service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have Log on as a service authority for the service to run correctly. If the user does not have Log on as a service authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of Log on as a service. The Installation wizard grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group. You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the `wasservice` command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol version 6 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the administrative agent process attempts to run, the service is unable to access the user environment variable that specifies IPv6, and thus, attempts to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the administrative agent process runs as the same user ID from which the environment variable that specifies IPv6 is defined, instead of as local system.

Default Windows service information

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is `automatic`. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than `automatic`, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a `startServer` command. For example, if you configure an application server as a Linux service and issue the `startServer` command, then the `wasservice` command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The tool displays the Profile creation summary panel.

16. Click **Create** to create the management profile for the administrative agent, or click **Back** to change the characteristics of the profile.

The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

When the profile creation completes, the tool displays the Profile creation complete panel.

17. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

With the First steps console, you can create additional profiles and start the application server.

Results

You created a management profile for the administrative agent.

Refer to the description of the **manageprofiles** command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Register application servers with the administrative agent using the `registerNode` command. Then, access the administrative agent console to administer your application servers.

Creating management profiles for job managers

You can create a management profile for the job manager to coordinate administrative actions among multiple deployment managers, administer multiple unfederated application servers, asynchronously submit jobs to start servers, and a variety of other tasks.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: **Solaris** When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root/.Xdefaults* file:

```
Eclipse*spacing:0  
Eclipse*fontList:-misc-fixed-medium-r-normal-*-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the product, you must create a profile. This procedure describes creating a management profile with a job manager server using the graphical user interface provided by the Profile Management Tool. You can also use the **manageprofiles** command to create a job manager. See the description of the **manageprofiles** command for more information.

You cannot create a management profile with a job manager that is enabled for the feature pack, as the profile has no requirements for feature-pack capability. However, you can use the profile in a feature-pack environment.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

1. Start the Profile Management Tool to create a new runtime environment.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

```
- Linux HP-UX Solaris AIX app_server_root/bin/  
ProfileManagement  
- Windows app_server_root\bin\ProfileManagement
```

The name of the command varies per platform:

```
- Linux HP-UX Solaris AIX pmt.sh  
- Windows pmt.bat
```

- Select the Profile Management Tool option from the First steps console.
- **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.

- **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click *the_operating_system_menus_to_access_programs > IBM WebSphere > your_product > Profile Management Tool*.
2. Click **Launch Profile Management Tool**, and then click **Create** on the Profiles tab to create a new profile.
The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.
The tool displays the Environment selection panel.
 3. Select **Management**, and click **Next**.
The Server type selection panel is displayed.
 4. Select **Job manager**. Click **Next**.
The Profile creation options panel is displayed.
 5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.
The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.
 6. If you selected **Typical profile creation**, go to the step on administrative security.
 7. If you selected **Advanced profile creation**, optionally select to deploy the administrative console, and then click **Next**.
If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.
The tool displays the Profile name and location panel.
 8. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

Profile naming guidelines: 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 * & ?
- Slashes (/) or (\)

The 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 only one profile exists on a machine, every command works on the single server process in the configuration. 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.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the

default profile. These commands use the `-profileName` parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

Default profile information

The default profile name is `<profile_type><profile_number>`:

- `<profile_type>` is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- `<profile_number>` is a sequential number that is used to create a unique profile name

AIX **HP-UX** **Linux** **Solaris** The default profile directory is `app_server_root/profiles`, where `app_server_root` is the installation root.

Windows The default profile directory is `app_server_root\profiles`, where `app_server_root` is the installation root.

9. On the Node, host, and cell names panel, specify a unique node name, the actual host name of the machine, and a unique cell name. Click **Next**.

Table 119. Characteristics of the job manager node.

This table shows the characteristics of the job manager node.

| Field Name | Default Value | Constraints | Description |
|------------|---|--|--|
| Node name | <p><i>shortHostName</i> JobMgr <i>NodeNumber</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>NodeNumber</i> is a sequential number starting at 01. | Use a unique name for the job manager. | The name is used for administration within the job manager cell. |
| Host name | The long form of the domain name server (DNS) name. | <p>The host name must be addressable through your network.</p> <p>Read about host name considerations.</p> | Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table. |

Table 119. Characteristics of the job manager node (continued).

This table shows the characteristics of the job manager node.

| Field Name | Default Value | Constraints | Description |
|------------|---|---|--|
| Cell name | <p><i>shortHostName</i> Cell <i>CellNumber</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>CellNumber</i> is a sequential number starting at 01. | <p>Use a unique name for the cell. If you plan to migrate a Version 5 cell to this Version 7, use the same cell name as the Version 5 cell. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a <code>javax.naming.NameNotFoundException</code> error, in which case, create uniquely named cells.</p> | <p>All federated nodes become members of the cell, which you name in this panel.</p> |

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path length

Windows The number of characters in the `profiles_directory_path\profile_name` directory must be less than or equal to 80 characters.

Host name considerations

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the `hostName` property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the `hostName` property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying characteristics, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.
12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports within the management profile for the job manager are unique, or intentionally conflicting, and click **Next**.

If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

Port conflict resolution

Ports are recognized as being in use if one of the following conditions exists:

- The ports are assigned to a profile created from an installation that is performed by the current user.
- The port is currently in use.

Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- **Linux** **HP-UX** **Solaris** **AIX** *profile_root/properties/portdef.props* file
- **Windows** *profile_root\properties\portdef.props* file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

Windows **Linux** The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the job manager process as a Windows service on a Windows operating system or as a Linux Service on a Linux operating system, and click **Next**.

The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the `WASService.exe` command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

Windows The product attempts to start Windows services for job manager processes that are started by a `startServer` command. For example, if you configure a job manager as a Windows service and issue the `startServer` command, then the `wasservice` command attempts to start the defined service.

If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have Log on as a service authority for the service to run correctly. If the user does not have Log on as a service authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of Log on as a service. The Installation wizard grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the `wasservice` command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6.0 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the job manager process tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the job manager process runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as local system.

Default Windows service information

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.

- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is automatic. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than automatic, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The tool displays the Profile Creation Summary panel.

16. Click **Create** to create the management profile for the job manager, or click **Back** to change the characteristics of the profile.

The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

When the profile creation completes, the tool displays the Profile creation complete panel.

17. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

With the First steps console, you can create additional profiles and start the application server.

Results

You created a management profile for the job manager.

Refer to the description of the **manageprofiles** command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Access the job manager console to perform a variety of administrative tasks. You can coordinate management actions among multiple deployment managers, administer multiple unfederated application servers, asynchronously submit jobs to start servers, and so on.

Creating secure proxy profiles

You can create a secure proxy profile to serve as the initial point of entry into your enterprise environment. Typically, a secure proxy server exists in the demilitarized zone (DMZ), accepts requests from clients on the Internet, and forwards the requests to servers in your enterprise environment.


Before you begin

Before you use the Profile Management Tool, install the core product files. You can create two different secure proxy profiles depending on which core product files you install. The core product files could either be for a Network Deployment installation or a DMZ Secure Proxy Server installation. Read about the profiles created for the different installations in About this task.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention:  When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root/.Xdefaults* file:

```
Eclipse*spacing:0  
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the product, you must create a profile. This procedure describes creating a secure proxy profile using the graphical user interface that is provided by the Profile Management Tool. You can also use the **manageprofiles** command to create a secure proxy profile. See the description of the **manageprofiles** command for more information.

You cannot create a secure proxy profile that is enabled for the feature pack, as the profile has no requirements for feature-pack capability. However, you can use the profile in a feature-pack environment.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can

optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

You can create two different profiles for the DMZ Secure Proxy Server using this task. You can create a secure proxy server profile on a Network Deployment installation. However, you can only configure this profile in a Network Deployment installation. To use the secure proxy server of the profile, you must export the profile from the Network Deployment environment and then import it into the DMZ Secure Proxy Server installation. Read about exporting and importing the secure proxy profile in the topic about the ConfigArchiveOperations command group for the AdminTask object. Alternatively, you can create a secure proxy server profile on a DMZ Secure Proxy Server installation. In this situation the secure proxy server does not have a Web container, and so cannot host an administrative console. To administer this secure proxy server, you must employ wsadmin scripting commands.

1. Start the Profile Management Tool to create a new runtime environment.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

```
- Linux HP-UX Solaris AIX app_server_root/bin/ProfileManagement
- Windows app_server_root\bin\ProfileManagement
```

The name of the command varies per platform:

```
- Linux HP-UX Solaris AIX pmt.sh
- Windows pmt.bat
```

- Select the Profile Management Tool option from the First steps console.
 - **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.
 - **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click **the_operating_system_menus_to_access_programs > IBM WebSphere > your_product > Profile Management Tool**.
2. Click **Create** to create a new profile.
 3. Click **Launch Profile Management Tool**, and then click **Create** on the Profiles tab to create a new profile.

The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

The tool displays the Environment selection panel.

4. Select **Secure proxy (configuration only)** for the Network Deployment image, or **Secure proxy** for the DMZ image, and click **Next**.

The Profile creation options panel is displayed.

5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.

6. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the administrative security.
7. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

Profile naming guidelines: 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 * & ?
- Slashes (/) or (\)

The 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 only one profile exists on a machine, every command works on the single server process in the configuration. 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.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the `-profileName` parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

Default profile information

The default profile name is `<profile_type><profile_number>`:

- `<profile_type>` is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- `<profile_number>` is a sequential number that is used to create a unique profile name

AIX **HP-UX** **Linux** **Solaris** The default profile directory is `app_server_root/profiles`, where `app_server_root` is the installation root.

Windows The default profile directory is `app_server_root\profiles`, where `app_server_root` is the installation root.

8. On the Node and Host Names panel, specify a unique node name, a server name, and the actual host name of the machine. Click **Next**.

Table 120. Characteristics of the secure proxy server node.

This table shows the characteristics of the secure proxy server node.

| Field name | Default value | Constraints | Description |
|-------------|--|--|--|
| Node name | <i>shortHostName</i> Node where: <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>NodeNumber</i> is a sequential number starting at 01. | Use a unique name for the secure proxy server. | The name is used for administration within the deployment manager cell. |
| Server name | proxy1 | Specifies a logical name for the server. Server names must be unique within a node. However, for multiple nodes within a cluster, you might have different servers with the same server name as long as the server and node pair are unique. | The server name is used for administration within the deployment manager cell. |
| Host name | The long form of the domain name server (DNS) name. | The host name must be addressable through your network. Read about host name considerations. | Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table. |

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path length

Windows The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Host name considerations

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, *localhost*, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name

that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the `hostName` property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the `hostName` property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying the node name, server name, and host name for the secure proxy profile, the tool displays the Security Level Selection panel.

9. Accept the defaults or change the proxy security level and the protocols, and click **Next**.

You can optionally change your security settings after you create the secure proxy server profile. Read about tuning security properties for the secured proxy server.

After displaying the security level options, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.
12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports within the secure proxy profile are unique, or intentionally conflicting, and click **Next**.

Port conflict resolution

Ports are recognized as being in use if one of the following conditions exists:

- The ports are assigned to a profile created from an installation that is performed by the current user.
- The port is currently in use.

Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- **Linux** **HP-UX** **Solaris** **AIX** `profile_root/properties/portdef.props` file
- **Windows** `profile_root\properties\portdef.props` file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the `updatePorts.ant` file by using the `ws_ant` script.

Windows **Linux** The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the secure proxy server as a Windows service on a Windows operating system or as a Linux Service on a Linux operating system, and click **Next**.

The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the `WASService.exe` command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

Windows The product attempts to start Windows services for secure proxy processes that are started by a `startServer` command. For example, if you configure a secure proxy server as a Windows service and issue the `startServer` command, then the `wasservice` command attempts to start the defined service.

If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have Log on as a service authority for the service to run correctly. If the user does not have Log on as a service authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of Log on as a service. The Installation wizard grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the `wasservice` command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6.0 (IPv6) if the service is configured to run as local system.

Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the secure proxy server process attempts to run, the service is unable to access the user environment variable that specifies IPv6, and thus attempts to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the secure proxy server process runs as the same user ID from which the environment variable that specifies IPv6 is defined, instead of as *Local System*.

Default Windows service information

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is automatic. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than automatic, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

The tool displays the Profile creation summary panel.

16. Click **Create** to create the secure proxy server profile, or click **Back** to change the characteristics of the profile.

The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

When the profile creation completes, the tool displays the Profile creation complete panel.

17. If the secure proxy profile that you are creating is part of the DMZ Secure Proxy Server for IBM WebSphere Application Server installation, optionally select **Launch the First steps console**. Click **Finish** to exit.

With the First steps console, you can create additional profiles, and start the application server.

If the secure proxy profile that you are creating is part of the Network Deployment installation, you do not have the option of launching the First steps console.

Results

Depending on your installation, you have either created a secure proxy server profile on a Network Deployment image or a secure proxy profile on a DMZ Secure Proxy Server installation.

Refer to the description of the **manageprofiles** command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

The secure proxy server can accept requests from clients on the Internet and forward the requests to servers in your enterprise environment.

The secure proxy profile is available both on the Network Deployment and the DMZ images. You cannot start the profile on the Network Deployment image. The profile is used only for configuration on an administrative console. After you configure the profile, you can export it and then import it into the secure proxy profile of the DMZ image. The secure proxy profile is fully operational on the DMZ image.

Creating cell profiles

You can create a cell profile in a single pass with the Profile Management Tool. This cell profile contains a federated application server node and a deployment manager.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from x to y . Assume that you are user x and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: **Solaris** When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the `app_server_root/.Xdefaults` file:

```
Eclipse*spacing:0  
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the Network Deployment product, you must create a profile. This procedure describes how to create a cell profile with the Profile Management Tool, which is a graphical user interface. You can also use the **manageprofiles** command to create a cell profile. See the description of the **manageprofiles** for more information.

If you additionally install the feature pack, you can use either the Profile Management Tool or the **manageprofiles** command to create a cell profile for the feature pack.

A cell profile contains a deployment manager profile and a federated application server node profile. You can federate additional Application Server node profiles into this deployment manager profile after initial creation of the cell profile.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

1. Start the Profile Management Tool to create a new runtime environment.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

```
- Linux HP-UX Solaris AIX app_server_root/bin/  
ProfileManagement  
- Windows app_server_root\bin\ProfileManagement
```

The name of the command varies per platform:

```
- Linux HP-UX Solaris AIX pmt.sh  
- Windows pmt.bat
```

- Select the Profile Management Tool option from the First steps console.
- **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.
- **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click

the_operating_system_menus_to_access_programs > IBM WebSphere > *your_product* > **Profile Management Tool**.

2. Click **Create** to create a new profile.
3. Click **Launch Profile Management Tool**, and then click **Create** on the Profiles tab to create a new profile.

The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

The tool displays the Environment selection panel.

4. Select **Cell with Feature Pack for SCA** if you want to create a cell profile for the Feature Pack for SCA, or **Cell** if you do not, and then click **Next**.

The Profile creation options panel is displayed.

5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.

6. If you selected **Typical profile creation**, go to the step on administrative security.
7. If you selected **Advanced profile creation**, then select the applications that you want to deploy, and click **Next**.

The tool displays the Profile name and location panel.

8. If you selected **Advanced profile creation**, then specify the deployment manager profile name, the application server profile name and the profile directory on the Profile name and location panel, or accept the defaults. Click **Next**.

Profile naming guidelines: 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 * & ?
- Slashes (/) or (\)

The 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 only one profile exists on a machine, every command works on the single server process in the configuration. 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.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the `-profileName` parameter if the profile is not the default profile. In those cases, it might be easier to use the commands that are in the `bin` directory of each profile. When you issue one of these commands within the `bin` directory of a profile, the command acts on that profile unless the `-profileName` parameter specifies a different profile.

Default profile information

The default profile name is `<profile_type><profile_number>`:

- `<profile_type>` is a value of AppSrv, Dmgr, Custom, AdminAgent, JobMgr, or SecureProxySrv.
- `<profile_number>` is a sequential number that is used to create a unique profile name

AIX **HP-UX** **Linux** **Solaris** The default profile directory is `app_server_root/profiles`, where `app_server_root` is the installation root.

Windows The default profile directory is `app_server_root\profiles`, where `app_server_root` is the installation root.

The tool then displays the Node, host, and cell names panel.

9. Specify a unique deployment manager node name, a unique application server node name, the actual host name of the machine, and a unique cell name for the cell, and click **Next**.

Table 121. Characteristics of the cell profile.

This table shows the characteristics of the cell profile.

| Field Name | Default Value | Constraints | Description |
|------------------------------|---|---|--|
| Deployment manager node name | <code>shortHostName</code> <code>CellManager</code> <code>NodeNumber</code> where: <ul style="list-style-type: none"> • <code>shortHostName</code> is the short host name. • <code>NodeNumber</code> is a sequential number starting at 01. | Use a unique name for the deployment manager. | The name is used for administration within the deployment manager cell. |
| Application server node name | <code>shortHostName</code> <code>Node</code> <code>NodeNumber</code> where: <ul style="list-style-type: none"> • <code>shortHostName</code> is the short host name • <code>NodeNumber</code> is a sequential number starting at 01 | Use a unique name for the application server. | The name is used for administration within the deployment manager cell. |
| Host name | The long form of the domain name server (DNS) name. | The host name must be addressable through your network. | Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table. |

Table 121. Characteristics of the cell profile (continued).

This table shows the characteristics of the cell profile.

| Field Name | Default Value | Constraints | Description |
|------------|---|--|---|
| Cell name | <p><i>shortHostName</i> Cell <i>CellNumber</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name. • <i>CellNumber</i> is a sequential number starting at 01. | <p>Use a unique name for the deployment manager cell. If you plan to migrate a Version 5 or Version 6 deployment manager cell to this Version 7 deployment manager, use the same cell name as the Version 5 or Version 6 deployment manager. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a <code>javax.naming.NameNotFoundException</code> error, in which case, create uniquely named cells.</p> | <p>All federated nodes become members of the deployment manager cell, which you name in this panel.</p> |

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Directory path considerations

Windows The number of characters in the `profiles_directory_path\profile_name` directory must be less than or equal to 80 characters.

Host name considerations

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, `localhost`, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the `hostName` property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the `hostName` property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After displaying the cell characteristics, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

If you installed the Samples, and you chose to deploy them, then the Samples require an account under which to run. Supply the Samples password for the account. You cannot change the user name of the account.

After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, then go to the step that displays the Profile summary panel.
12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports specified for the deployment manager are unique, and click **Next**.

If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

Port conflict resolution

Ports are recognized as being in use if one of the following conditions exists:

- The ports are assigned to a profile created from an installation that is performed by the current user.
- The port is currently in use.

Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- **Linux** **HP-UX** **Solaris** **AIX** `profile_root/properties/portdef.props` file
- **Windows** `profile_root\properties\portdef.props` file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the `updatePorts.ant` file by using the `ws_ant` script.

15. Verify that the ports specified for the application server are unique, and click **Next**.

The same discussion on ports in the previous step applies to this step.

Windows **Linux** The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

16. Choose whether to run the application server as a Windows service on a Windows operating system or as a Linux service on a Linux operating system, then click **Next**.

• **Windows**
The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the `WASService.exe` command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

Windows The product attempts to start Windows services for application server processes that are started by a `startServer` command. For example, if you configure an application server as a Windows service, and issue the `startServer` command, then the `wasservice` command attempts to start the defined service.

If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have Log on as a service authority for the service to run correctly. If the user does not have Log on as a service authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of Log on as a service. The Installation wizard grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the `wasservice` command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the product tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus, tries to start as Internet Protocol Version 4 (IPv4). The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the product runs with the same user ID from which the environment variable that specifies IPv6 is defined, instead of as local system.

Default values for the Windows service

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is automatic. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than automatic, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux

The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

If you previously selected **Advanced profile creation**, the next panel displays the Web server definition panel.

17. For advanced profile creation, if you choose to include a Web server definition in the profile now, specify the Web server characteristics on the panels, and click **Next** until you complete the Web server definition panels.

If you use a Web server to route requests to the product, then you need to include a Web server definition. You can include the definition now, or define the Web server to the product later. If you define the Web server definition during the creation of this profile, then you can install the Web server and its plug-in after you create the profile. However, you must install both to the paths that you specify on the Web server definition panels. If you define the Web server to the product after you create this profile, then you must define the Web server in a separate profile.

The tool displays the Profile Creation Summary panel.

18. Click **Create** to create the cell profile, or click **Back** to change the characteristics of the cell profile.

The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

When the profile creation completes, the tool displays the Profile creation complete panel.

19. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

With the First steps console, you can create additional profiles and start the application server.

Results

You created a cell profile.

Refer to the description of the **manageprofiles** command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

Creating custom profiles

Create a custom profile so that you can include application servers, clusters, or other Java processes, such as a messaging server, in its empty node. You can use the Profile Management Tool to create a custom profile.

Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the SetPermissions utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention: **Solaris** When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *app_server_root/.Xdefaults* file:

```
Eclipse*spacing:0  
Eclipse*fontList:-misc-fixed-medium-r-normal-*-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the Network Deployment product, you must create a profile. This topic describes creating a custom profile using the Profile Management Tool. A custom profile is an empty node that you can customize to include application servers, clusters, or other Java processes, such as a messaging server.

You can also use the **manageprofiles** command to create a custom profile. See the description of the **manageprofiles** for more information.

If you additionally install the feature pack, you can use either the Profile Management Tool or the **manageprofiles** to create a custom profile for the feature pack.

By default, the Profile Management Tool federates a custom node when you create a custom profile. Federating the node makes the node operational. You must have access to a running deployment manager to federate the node. Otherwise, a connection error displays. You can federate the node later if you do not have access to a running deployment manager, or for any other reason.

If the custom profile is on a machine that does not have a deployment manager, then the deployment manager must be accessible over the network to support the federation of the node.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

1. Install the product to create the core product files.
2. Start the Profile Management Tool to create a new runtime environment.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

- **Linux** **HP-UX** **Solaris** **AIX** `app_server_root/bin/ProfileManagement`
- **Windows** `app_server_root\bin\ProfileManagement`

The name of the command varies per platform:

- **Linux** **HP-UX** **Solaris** **AIX** `pmt.sh`
- **Windows** `pmt.bat`

- Select the Profile Management Tool option from the First steps console.
 - **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.
 - **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click *the_operating_system_menus_to_access_programs* > **IBM WebSphere > your_product > Profile Management Tool**.
3. Click **Create** to create a new profile.
 4. Click **Launch Profile Management Tool**, and then click **Create** on the Profiles tab to create a new profile.

The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

The tool displays the Environment selection panel.

5. Select **Custom profile with Feature Pack for SCA** if you want to create a cell profile for the Feature Pack for SCA, or **Custom profile** if you do not, and then click **Next**.

The Profile creation options panel is displayed.

6. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.

7. If you selected **Typical profile creation**, then go to the step on federating the node.
8. If you selected **Advanced profile creation**, then specify the custom profile name and the profile directory on the Profile name and location panel, or accept the defaults, and click **Next**.

Profile naming guidelines: 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 `*&?`
- Slashes (`/`) or (`\`)

The 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 only one profile exists on a machine, every command works on the single server process in the configuration. 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.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the `-profileName` parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

Default profile information

The default profile name is `<profile_type><profile_number>`:

- `<profile_type>` is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- `<profile_number>` is a sequential number that is used to create a unique profile name

AIX **HP-UX** **Linux** **Solaris** The default profile directory is `app_server_root/profiles`, where `app_server_root` is the installation root.

Windows The default profile directory is `app_server_root\profiles`, where `app_server_root` is the installation root.

The tool then displays the Node and host names panel.

9. Specify the node and host characteristics for the custom profile, and click **Next**.

Migration considerations

If you plan to migrate an installation of Network Deployment Version 5 or Version 6 to Version 7, then use the same cell name for the Version 7 deployment manager that you used for the Version 5 or Version 6 cell. A cell name must be unique in any circumstance in which the product is running on the same physical machine or cluster of machines, such as a sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names must also be unique if their namespaces are federated. Otherwise, you might encounter symptoms such as a `javax.naming.NameNotFoundException` error, in which case, create uniquely named cells.

After migrating the cell, the Version 5 or Version 6 managed nodes are now managed by the Version 7 deployment manager in compatibility mode. You can migrate individual Version 5 or Version 6 managed nodes in the cell to Version 7. To do so, you must create a Version 7 profile with the same node name as the Version 5 or Version 6 managed node.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Table 122. Characteristics of the custom profile.

This table shows the characteristics of the custom profile.

| Field Name | Default Value | Constraints | Description |
|------------|---|---|---|
| Node name | <p><i>shortHostName</i> Node <i>NodeNumber</i></p> <p>where:</p> <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name • <i>NodeNumber</i> is a sequential number starting at 01 | <p>Avoid using the reserved terms.</p> <p>Use a unique name within the deployment manager cell.</p> <p>If you plan to migrate a Version 5 or Version 6 managed node, then use the same node name for this Version 7 custom profile.</p> | <p>The name is used for administration within the deployment manager cell to which the custom profile is added. Use a unique name within the deployment manager cell.</p> <p>After migrating a Version 5 or Version 6 deployment manager cell to a Version 7 deployment manager, you can migrate the Version 5 or Version 6 custom profiles that are running in compatibility mode in the Version 7 deployment manager.</p> |
| Host name | The long form of the domain name server (DNS) name. | The host name must be addressable through your network. | Use the actual DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name that follows this table. |

Directory path considerations

Windows The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Host name considerations

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, *localhost*, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS) look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the *hostName* property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as *xmachine.manhattan.ibm.com*

- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the `hostName` property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After specifying custom profile characteristics, the tool displays the Federation panel.

10. If administrative security is enabled for the deployment manager, specify the host name and SOAP port of the deployment manager, and the user name and password for the deployment manager. Click **Next**.

After federation, the process in the custom profile is the node agent process. The node agent process is the agent of the deployment manager for the custom node. The node agent responds to commands from the deployment manager to perform tasks that include the following actions:

- Creating application server processes, clusters, and cluster members
- Starting and stopping application server processes
- Synchronizing configurations between the current edition on the deployment manager and the copy that exists on the node
- Deleting application server processes

Should you federate the node?

The recommendation is that you federate the custom node at this time. The deployment manager must be running and accessible when you click **Next** on the Federation panel to federate the custom node. If the custom profile is on a machine that does not have a deployment manager, then the deployment manager must be running and accessible over the network to allow the federation of the node. If the deployment manager is not running or not accessible before you click **Next**, but you can start it and make it accessible at this time, then do so. Otherwise, select the **Federate the node later** check box.

If you are unsure whether the deployment manager is running or accessible, then do not federate now. Federate the node when you can verify the availability of the deployment manager.

A possibility exists that the deployment manager is reconfigured to use the non-default remote method invocation (RMI) as the preferred Java Management Extensions (JMX) connector. Click **System Administration > Deployment manager > Administrative services** in the administrative console of the deployment manager to verify the preferred connector type.

If RMI is the preferred JMX connector, then you must use the `addNode` command to federate the custom profile later. Use the `addNode` command so that you can specify the JMX connector type and the RMI port.

If the deployment manager uses the default SOAP JMX connector type, specify the host name and SOAP port and federate the node now to create a functional node that you can customize.

Federating when the deployment manager is not available

If you federate a custom node when the deployment manager is not running or is not accessible, then an error message is displayed. If the deployment manager becomes unavailable during the profile creation process, then the installation indicator in the logs is `INSTCONFFAIL`, to indicate a complete failure. The resulting custom profile is unusable. You must delete the profile. Read about deleting a profile for more information.

If you chose to federate now, and you previously selected **Advanced profile creation**, then the Security certificate panel displays next. Go to the step on creating and importing certificates.

Otherwise, the Profile Creation Summary panel displays for the typical profile creation option. Go to the step on creating the custom profile.

11. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

12. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including `PKCS12`, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are `key.p12`, `trust.p12`, `root-key.p12`, `default-signers.p12`, `deleted.p12`, and `ltpa.jceks`. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The `key.p12` file contains the default personal certificate. The `trust.p12` file contains the signer certificate from the default root certificate. The `root-key.p12` file contains the

root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other. An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

13. Verify that the ports within the custom profile are unique, or intentionally conflicting, and click **Next**.

Port conflict resolution

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- **Linux** **HP-UX** **Solaris** **AIX** `profile_root/properties/portdef.props` file
- **Windows** `profile_root\properties\portdef.props` file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the updatePorts.ant file by using the ws_ant script.

The Profile Creation Summary panel is displayed.

14. Click **Create** to create the custom profile, or click **Back** to change the characteristics of the custom profile.

If you previously chose to federate the custom node on the Federation panel, the deployment manager had to be running and accessible. The deployment manager must be running and accessible when you click **Create**. If you think the deployment manager might no longer be running or might have become inaccessible, then start the deployment manager and make it accessible, or make it accessible if it is already running.

The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

When the profile creation completes, the tool displays the Profile creation complete panel.

15. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

With the First steps console, you can create additional profiles and start the application server.

Results

You created a custom profile. The node within the profile is empty until you federate the node and use the deployment manager to customize the node.

The directory structure shows the new profile folder within the profiles directory. The profile folder has the same name as the profile that you create.

Refer to the description of the **manageprofiles** command to learn about creating a profile using a command instead of the Profile Management Tool.

The Profile Management Tool creates a log during profile creation. The logs are in the `install_dir/logs/manageprofiles` directory. The files are named in this pattern: `manageprofiles_create_profile_name.log`.

What to do next

Federate the node into the deployment manager cell if you did not already do so when you created the node. Then, use the deployment manager to create an application server on the node.

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

Creating application server profiles

Create an application server profile so that you can make applications available to the Internet or to an intranet, typically using Java technology. You can create an application server profile using the Profile Management Tool.


Before you begin

Before you use the Profile Management Tool, install the product files.

The Profile Management Tool is the graphical user interface for the **manageprofiles** command. See the description of the **manageprofiles** command for more information.

You must provide enough system temporary space to create a profile. For information, read about the file system requirements for profiles.

Attention: When you launch the Profile Management Tool, the tool could lock up in the following situation for a non-root user: Log into a machine as root, use the `SetPermissions` utility to change the user from *x* to *y*. Assume that you are user *x* and log back into the machine. Launch the Profile Management Tool, click **Profile Management Tool**, and click **Create**. The next click after the click on **Create** could lock up the tool.

Attention:  When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the `app_server_root/.Xdefaults` file:

```
Eclipse*spacing:0  
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before launching the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

About this task

After installing the core product files for the Network Deployment product, you must create a profile. This procedure describes creating an application server profile using the graphical user interface provided by the Profile Management Tool.

You can also use the **manageprofiles** command to create an application server profile. See the description of the **manageprofiles** command for more information.

If you additionally install the feature pack, you can use either the Profile Management Tool or the **manageprofiles** to create an application server profile for the feature pack.

An application server profile has a default server, which is **server1**, the default application that includes the Snoop servlet and the Hitcount servlet, and application Samples. You can federate the application server or use it as a standalone application server.

You can create profiles with the Profile Management Tool using the typical profile creation process or the advanced profile creation process. The typical profile creation process uses default settings and assigns unique port values. You can optionally set values as allowed. For the advanced profile creation process you can accept the default values, or specify your own values.

1. Start the Profile Management Tool to create a new runtime environment.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

```
– Linux HP-UX Solaris AIX app_server_root/bin/ProfileManagement
– Windows app_server_root\bin\ProfileManagement
```

The name of the command varies per platform:

```
– Linux HP-UX Solaris AIX pmt.sh
– Windows pmt.bat
```

- Select the Profile Management Tool option from the First steps console.
 - **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.
 - **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click **the_operating_system_menus_to_access_programs > IBM WebSphere > your_product > Profile Management Tool**.
2. Click **Create** to create a new profile.
 3. Click **Launch Profile Management Tool**, and then click **Create** on the Profiles tab to create a new profile.

The Profiles tab contains a list of profiles that have been created on your machine. No action can be done on a selected profile unless the profile can be augmented. The Augment button is greyed out unless a profile that you select can be augmented.

The tool displays the Environment selection panel.

4. Select the type of application server profile that you want to create, and click **Next**.
 - Select **Application server** if you want to create an application server profile that is not enabled for the feature pack.
 - Select **Application server with Feature Pack for SCA** if you want to create an application server profile that is enabled for the Feature Pack for SCA.

The Profile creation options panel is displayed.

5. Select either **Typical profile creation** or **Advanced profile creation**, and click **Next**.

The **Typical profile creation** option creates a profile that uses default configuration settings. With the **Advanced profile creation** option, you can specify your own configuration values for a profile.

6. If you selected **Typical profile creation**, then go to the step on administrative security.
7. If you selected **Advanced profile creation**, then select the applications that you want to deploy; and click **Next**.

The tool displays the Profile name and location panel.

8. Specify a name for the profile and the directory path for the profile directory, or accept the default values. Then, click **Next**.

Profile naming guidelines: 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 * & ?
- Slashes (/) or (\)

The 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 only one profile exists on a machine, every command works on the single server process in the configuration. 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.

Addressing a profile in a multiprofile environment

When multiple profiles exist on a machine, certain commands require that you specify the profile to which the command applies if the profile is not the default profile. These commands use the `-profileName` parameter to identify which profile to address. You might find it easier to use the commands that are in the `bin` directory of each profile.

Use these commands to query the command shell to determine the calling profile and to address these commands to the calling profile.

Default profile information

The default profile name is `<profile_type><profile_number>`:

- `<profile_type>` is a value of `AppSrv`, `Dmgr`, `Custom`, `AdminAgent`, `JobMgr`, or `SecureProxySrv`.
- `<profile_number>` is a sequential number that is used to create a unique profile name

AIX **HP-UX** **Linux** **Solaris** The default profile directory is `app_server_root/profiles`, where `app_server_root` is the installation root.

Windows The default profile directory is `app_server_root\profiles`, where `app_server_root` is the installation root.

9. On the Node and host names panel, specify the characteristics for the application server, and click **Next**.

Use unique names for each application server that you create.

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following terms are reserved folder names:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Some default values in the following table are split on multiple lines for printing purposes.

| Field Name | Default Value | Constraints | Description |
|-------------|---|---|--|
| Node name | <i>shortHostName</i> Node <i>NodeNumber</i> where: <ul style="list-style-type: none"> • <i>shortHostName</i> is the short host name • <i>NodeNumber</i> is a sequential number starting at 01 | Avoid using the reserved terms. | Select any name you want. To help organize your installation, use a unique name if you plan to create more than one application server on the machine. |
| Server name | server1 | Use a unique name for the application server. | The name is a logical name for the application server. |
| Host name | The long form of the domain name server (DNS) name. | Addressable through your network. | Use the DNS name or IP address of your machine to enable communication with your machine. See additional information about the host name following this table. |

Node name considerations: If you plan to migrate an installation of Version 5 or Version 6 Network Deployment to Version 7 and migrate one of the managed nodes in the cell, use the same node name for the Version 7 application server that you used for the Version 5 or Version 6 managed node.

Windows **Directory path considerations:** The installation directory path must be less than or equal to 60 characters.

Host name considerations:

The host name is the network name for the physical machine on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and communicate with this node. Selecting a host name that other machines can reach within your network is important. Do not use the generic identifier, *localhost*, for this value. Also, do not attempt to install WebSphere Application Server products on a machine with a host name that uses characters from a double-byte character set (DBCS). DBCS characters are not supported when used in the host name.

If you define coexisting nodes on the same computer with unique IP addresses, then define each IP address in a domain name server (DNS)

look-up table. Configuration files for standalone application servers do not provide domain name resolution for multiple IP addresses on a machine with a single network address.

The value that you specify for the host name is used as the value of the `hostName` property in configuration documents for the standalone application server. Specify the host name value in one of the following formats:

- Fully qualified domain name server (DNS) host name string, such as `xmachine.manhattan.ibm.com`
- The default short DNS host name string, such as `xmachine`
- Numeric IP address, such as `127.1.255.3`

The fully qualified DNS host name has the advantages of being unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the application server configuration. This value for the host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is dependency on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added function of being redefined in the local hosts file so that the system can run the application server, even when disconnected from the network. To run disconnected, define the short name as the loopback address, `127.0.0.1`, in the hosts file to run disconnected. A disadvantage of this format is a dependency on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node that you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the `hostName` property in Express configuration documents whenever you change the machine IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

After specifying application server characteristics, the tool displays the Administrative security panel.

10. Optionally enable administrative security, and click **Next**.

You can enable administrative security now during profile creation, or later from the console. If you enable administrative security now, then enter a user name and password to log onto the administrative console.

If you installed the Samples, and you chose to deploy them, then the Samples require an account under which to run. Supply the Samples password for the account. You cannot change the user name of the account.

After specifying security characteristics, the tool displays the Security certificate panel if you previously selected **Advanced profile creation**.

11. If you selected **Typical profile creation** at the beginning of these steps, go to the step that displays the Profile summary panel.
12. Create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

Note: When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file.

If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

13. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. You should change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are key.p12, trust.p12, root-key.p12, default-signers.p12, deleted.p12, and ltpa.jceks. These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify. The key.p12 file contains the default personal certificate. The trust.p12 file contains the signer certificate from the default root certificate. The root-key.p12 file contains the root signing certificate. The default-signer.p12 file contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate is in the default-signer.p12 keystore file. The deleted.p12 keystore file is used to hold certificates deleted with the deleteKeyStore task so that they can be recovered if needed. The ltpa.jceks file contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

After displaying the Security certificate panels, the tool displays the Ports panel if you previously selected **Advanced profile creation**.

14. Verify that the ports specified for the standalone application server are unique, and click **Next**.

If you chose not to deploy the administrative console, then the administrative console ports are disabled on the Ports panel.

Port conflict resolution

Ports are recognized as being in use if one of the following conditions exists:

- The ports are assigned to a profile created from an installation that is performed by the current user.
- The port is currently in use.

Validation of ports occurs when you access the Port value assignment panel. Conflicts can still occur between the Port value assignment panel and the Profile creation complete panel because ports are not assigned until profile creation completes.

If you suspect a port conflict, then you can investigate the port conflict after the profile is created. Determine the ports that are used during profile creation by examining the following files.

- **Linux** **HP-UX** **Solaris** **AIX** `profile_root/properties/portdef.props` file
- **Windows** `profile_root\properties\portdef.props` file

Included in this file are the keys and values that are used in setting the ports. If you discover ports conflicts, then you can reassign ports manually. To reassign ports, run the `updatePorts.ant` file by using the `ws_ant` script.

Windows **Linux** The tool displays the Windows service definition panel if you are installing on a Windows operating system and the installation ID has the administrative group privilege. The tool displays the Linux service definition panel if you are installing on a supported Linux operating system and the ID that runs the Profile Management Tool is the root user.

15. Choose whether to run the application server as a Windows service on a Windows operating system or as a Linux service on a Linux operating system, then click **Next**.

- **Windows**
The Windows service definition panel is displayed for the Windows operating system only if the ID that installs the Windows service has the administrator group privilege. However, you can run the `WASService.exe` command to create the Windows service as long as the installer ID belongs to the administrator group. Read about automatically restarting server processes for more information.

Windows The product attempts to start Windows services for application server processes that are started by a `startServer` command. For example, if you configure an application server as a Windows service, and issue the `startServer` command, then the `wasservice` command attempts to start the defined service.

If you chose to install a local system service, then you do not have to specify your user ID or password. If you create a specified user type of service, then you must specify the user ID and the password for the user who runs the service. The user must have Log on as a service authority for the service to run correctly. If the user does not have Log on as a service authority, then the Profile Management tool automatically adds the authority.

To perform this profile creation task, the user ID must not contain spaces. In addition to belonging to the administrator group, the ID must also have the advanced user right of Log on as a service. The Installation wizard grants the user ID the advanced user right if the user ID does not already have the advanced user right and if the user ID belongs to the administrator group.

You can also create other Windows services after the installation is complete to start other server processes. Read about automatically restarting server processes for more information.

You can remove the Windows service that is added during profile creation during profile deletion. You can also remove the Windows service with the `wasservice` command.

IPv6 considerations

Profiles created to run as a Windows service fail to start when using Internet Protocol Version 6 (IPv6) if the service is configured to run as local system. Create a user-specific environment variable to enable IPv6. Since this environment variable is a user variable instead of a local system

variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as local system. When the Windows service for the product tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus, tries to start as Internet Protocol Version 4 (IPv4). The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the Windows service for the product runs with the same user ID from which the environment variable that specifies IPv6 is defined, instead of as local system.

Default values for the Windows service

Windows The following default values for the Windows service definition panel exist:

- The default is to run as a Windows service.
- The service process is selected to run as a system account.
- The user account is the current user name. User name requirements are the requirements that the Windows operating system imposes for a user ID.
- The startup type is automatic. The values for the startup type are those values that the Windows operating system imposes. If you want a startup type other than automatic, you can either select another available option from the menu or change the startup type after you create the profile. You can also remove the created service after profile creation, and add it later with the desired startup type. You can choose not to create a service at profile creation time and optionally create the service later with the desired startup type.

Linux

The Linux service definition panel is displayed if the current operating system is a supported version of Linux operating systems, and the current user has the appropriate permissions.

The product attempts to start Linux services for application server processes that are started by a startServer command. For example, if you configure an application server as a Linux service and issue the startServer command, then the **wasservice** command attempts to start the defined service.

By default, the product is not selected to run as a Linux service.

To create the service, the user that runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, then the Linux service definition panel is not displayed, and no service is created.

When you create a Linux service, you must specify a user name from which the service runs.

To delete a Linux service, the user must be the root user or have appropriate privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service for the user.

If you previously selected **Advanced profile creation**, the next panel displays the Web server definition panel.

16. For advanced profile creation, if you choose to include a Web server definition in the profile now, specify the Web server characteristics on the panels, and click **Next** until you complete the Web server definition panels.

If you use a Web server to route requests to the product, then you need to include a Web server definition. You can include the definition now, or define the Web server to the product later. If you define the Web server definition

during the creation of this profile, then you can install the Web server and its plug-in after you create the profile. However, you must install both to the paths that you specify on the Web server definition panels. If you define the Web server to the product after you create this profile, then you must define the Web server in a separate profile.

The tool displays the Profile Creation Summary panel.

17. Click **Create** to create the application server, or click **Back** to change the characteristics of the application server.

The Profile creation progress panel, which shows the configuration commands that are running, is displayed.

When the profile creation completes, the tool displays the Profile creation complete panel.

18. Optionally, select **Launch the First steps console**. Click **Finish** to exit.

With the First steps console, you can create additional profiles and start the application server.

Results

You created an application server profile. The node within the profile has an application server named server1.

Refer to the description of the **manageprofiles** command to learn about creating a profile using a command instead of the Profile Management Tool.

What to do next

Deploy an application to get started.

Read about fast paths for the product to get started deploying applications.

When you create the application server profile, a default server1 process is created. You can federate the server1 node into the deployment manager cell with the **addNode** command or from the administrative console of the deployment manager. The server1 process must be running to begin the federation from the deployment manager.

If you include all of the applications from the application server, then the act of federation installs the applications on the deployment manager where they can be redeployed.

Augmenting profiles using the graphical user interface

After completing the installation of a feature pack, a feature pack might require you to augment a profile to make that profile compatible with a particular feature pack. You can use the Profile Management Tool to augment a profile.

Before you begin

Before you use the Profile Management Tool, install the product files.

Augmenting existing profiles might result in changes to the profile configuration. Before augmenting a profile, back up the existing configuration in case you need to restore the configuration. Use the `backupConfig` command to back up your current configuration.

Each profile has one log file for augmentation. The augmentation log, if it exists, is overwritten if you augment the profile more than once. Optionally save the contents of the augmentation log before you start the next augmentation. You can choose the method of saving the log, such as renaming or copying the file. The augmentation log is located at

- **Linux** **HP-UX** **Solaris** **AIX** `app_server_root/logs/manageprofiles/profile_name_augment.log`
- **Windows** `app_server_root\logs\manageprofiles\profile_name_augment.log`

The feature pack allows you to create and augment certain profiles in one pass through the Profile Management Tool. For those profiles, use the **create** option in the Profile Management Tool to create a profile enabled for the feature pack instead of creating a Network Deployment profile and then augmenting the profile for the feature pack.

About this task

When you apply a feature pack, the feature pack might require augmentation of Network Deployment profiles to use the new capabilities. Use this task to augment these profiles.

For this feature pack, you can augment the application server profile, the management profile with a server type of deployment manager, the custom profile, and the cell profile of the Network Deployment product. You cannot augment the management profile with a server type of administrative agent, the management profile with a server type of job manager or the secure proxy profile. You can also create a new application server profile, a new deployment manager profile, a new cell profile, or a new custom profile that is enabled for the feature pack. Use the profile creation tasks to create these profiles.

This task describes how to augment a profile by using the Profile Management Tool. You can also use the **manageprofiles** command to augment a profile.

1. Back up the existing configuration using the backupConfig command if you have not already done so.
2. Start the Profile Management Tool.

You can use one of the following ways to start the tool.

- At the end of installation, select the check box to launch the Profile Management Tool.
- Issue the command directly from a command prompt.

The command is in the following directory:

- **Linux** **HP-UX** **Solaris** **AIX** `app_server_root/bin/ProfileManagement`
- **Windows** `app_server_root\bin\ProfileManagement`

The name of the command varies depending on the operating system:

- **Linux** **HP-UX** **Solaris** **AIX** `pmt.sh`
- **Windows** `pmt.bat`

- Select the Profile Management Tool option from the First steps console.
- **Windows** Use the **Start** menu to access the Profile Management Tool. For example, click **Start > Programs** or **All Programs > IBM WebSphere > your_product > Profile Management Tool**.
- **Linux** Use the Linux operating system menus used to start programs to start the Profile Management Tool. For example, click

the_operating_system_menus_to_access_programs > IBM WebSphere > *your_product* > Profile Management Tool.

3. Click **Launch Profile Management Tool**.
4. Select the profile that you want to augment.
5. Click **Augment**.
6. Select the augmentation that you want to apply to the profile, and click **Next**.
7. Click **Augment** on the summary panel.
8. When augmentation is complete, click **Finish**.

Results

You have augmented a profile.

Managing profiles for non-root users

The non-root can receive permissions for files and directories so that the non-root user can create and augment a profile.

Before you begin

This task assumes a basic familiarity with the **manageprofiles** command, the Profile Management Tool, and system commands.

This task uses the following terms:

- *Root users* refers to:
 - Linux HP-UX Solaris AIX Root users
 - Windows Administrators
- *Non-root users* refers to:
 - Linux HP-UX Solaris AIX Non-root users
 - Windows Non-administrators
- *Installer* refers to a root user or a non-root user.

Remember: An ease-of-use limitation exists for non-root users who create profiles. Mechanisms within the Profile Management Tool that suggest unique names and port values are disabled for non-root users. The non-root user must change the default field values in the Profile Management Tool for the profile name, node name, cell name, and port assignments. Consider assigning non-root users a range of values for each of the fields. You can assign responsibility to the non-root users for adhering to their assigned value ranges and for maintaining the integrity of their own definitions.

About this task

Non-root users might typically need these tasks completed so that they can start their own application servers in development environments. For instance, an application developer might test an application on an application server in a profile assigned to that application developer.

- Create a profile as an installer and assign ownership to a non-root user.

This topic describes how the installer creates and augments a profile, and assigns ownership of the profile directory to a non-root user so that the non-root user can start the application server for a specific profile.

- Grant write permission of files and directories to a non-root user for profile creation.
This topic describes how an installer authorizes a group to access certain files and directories so that non-root users in the group can create and augment profiles.
- Install maintenance as an installer and change the ownership of profile-related files.
This topic describes how to install product maintenance and change the ownership of new profile files to the non-root user that owns the profile. The installer changes ownership of the files so that the non-root user can then successfully start the application server.

Results

Depending on the tasks that the installer followed, the installer has completed the following actions:

- Created and optionally augmented a profile for a non-root user and assigned ownership of the profile directory to the non-root user
- Granted permission to the appropriate directories so that non-root users can create and augment profiles
- After installing maintenance, changed ownership of new profile files in a directory that is owned by a non-root user, so that the non-root user can successfully start the application server

What to do next

Depending on the tasks that the installer completes, a non-root user can create and augment a profile, start WebSphere Application Server, or do both.

Assigning profile ownership to a non-root user

An installer can create and augment a profile, and assign ownership of the profile directory to a non-root user so that the non-root user can start the product for a specific profile. Use this example to accomplish the tasks through commands.

Before you begin

This task assumes a basic familiarity with the **manageprofiles** command and system commands.

This task uses the following terms:

- *Root users* refers to:
 - Linux HP-UX Solaris AIX Root users
 - Windows Administrators
- *Non-root users* refers to:
 - Linux HP-UX Solaris AIX Non-root users
 - Windows Non-administrators
- *Installer* refers to a root user or a non-root user.

Before you can create and augment a profile, you must install the product.

About this task

An installer must perform the following steps to create, optionally augment a profile, and assign ownership for the profile directory and the logs directory. The ownership is assigned to a non-root user ID that is different from the installer ID. The non-root user needs access to these directories to start the product.

If augmentation of a particular profile is supported, then the installer might need to create a profile and later augment that profile for a feature pack. However, as the installer, create a feature pack-enabled profile when possible. To create a feature pack-enabled profile, use the appropriate feature-pack profile template, and skip the augmentation step.

The installer might have already completed the steps in this task to create a profile for a non-root user and changed ownership of particular directories to the non-root user. If you, as the installer, must now augment the profile for a non-root user, then begin with the step on augmentation.

For more information, see the topic on augmentation rules and limitations for feature packs.

This example creates a default profile.

The commands are split on multiple lines for printing purposes.

1. Create the profile by issuing the following code from a command prompt:

```
Linux HP-UX Solaris AIX  
./manageprofiles.sh -create -profileName profile01 -profilePath  
app_server_root/profiles/profile01 -templatePath  
app_server_root/profileTemplates/management -serverType DEPLOYMENT_MANAGER
```

```
Windows  
manageprofiles.bat -create -profileName profile01 -profilePath  
app_server_root/profiles/profile01 -templatePath  
app_server_root/profileTemplates/management -serverType DEPLOYMENT_MANAGER
```

2. Optionally augment the profile.

You must complete this step if the feature pack requires you to augment the profile that you created in the previous step to use the feature-pack capabilities.

```
Linux HP-UX Solaris AIX  
./manageprofiles.sh -augment -profileName profile01 -templatePath  
app_server_root/profileTemplates/SCA/dmgr.scafep
```

```
Windows  
manageprofiles.bat -augment -profileName profile01 -templatePath  
app_server_root/profileTemplates/SCA/dmgr.scafep
```

3. Change ownership of the profile01 profile directory to the user1 non-root user.

```
Linux HP-UX Solaris AIX For example, issue the following  
command:
```

```
chown -R user1 app_server_root/profiles/profile01
```

```
Windows Follow instructions in the Windows documentation to grant user1  
access to the following directory:
```

```
app_server_root/profiles/profile01
```

4. Change the ownership of the logs directory for the profile01 profile to the user1 non-root user to prevent displaying log messages to the console.

```
Linux HP-UX Solaris AIX Issue the following command:  
chown -R user1 app_server_root/logs/manageprofiles/profile01
```

Windows Follow instructions in the Windows documentation to grant user1 access to the following directory:

```
app_server_root\logs\manageprofiles\profile01
```

Results

The installer has created a default profile, optionally augmented the profile, and changed ownership of the profile directory and log directory to a non-root user.

What to do next

As the installer, you can continue to create and augment profiles, and assign ownership to non-root users as needed.

A non-root user ID can manage multiple profiles. Have the same non-root user ID manage an entire profile, whether it is the deployment manager profile, a profile that contains the application servers and the node agent, or a custom profile. A different user ID can be used for each profile in a cell, whether global security or administrative security is enabled or disabled. The user IDs can be a mix of root and non-root user IDs. For example, the root user might manage the deployment manager profile, while a non-root user might manage a profile that contains application servers and the node agent, or vice versa. However, typically, a root user or a non-root user manages all profiles in a cell.

The non-root user can use the same tasks to manage a profile that the root user uses.

Granting write permission for profile-related tasks

The installer can grant write permission of the appropriate files and directories to a non-root user. The non-root user can then create and augment the profile. The installer can create a group for users who are authorized to create and augment profiles, or the installer can give individual users the authority to create and augment profiles. The following example shows how to create a group that is authorized to create and augment profiles.

Before you begin

This task assumes a basic familiarity with system commands.

This task uses the following terms:

- *Root users* refers to:
 - **Linux** **HP-UX** **Solaris** **AIX** Root users
 - **Windows** Administrators
- *Non-root users* refers to:
 - **Linux** **HP-UX** **Solaris** **AIX** Non-root users
 - **Windows** Non-administrators
- *Installer* refers to a root user or a non-root user.

About this task

The steps that you follow to grant write permission of files and directories to a non-root user for profile creation and augmentation depends on whether a profile was previously created.

If at least one profile was created prior to implementing the following steps, then certain directories and files were created. Because these directories and files were created, skip the steps that create these directories and files. If no profile was previously created, then you must complete the steps to create the required directories and files. In most cases, a profile has been created previously.

The installer can perform the following steps to create the profilers group and give the group appropriate permissions to create and augment a profile.

1. Log on as the installer to the system where the product is installed.
2. Create the profilers group that you can use to create and augment profiles.
Read the documentation for your operating system for information about how to create groups.
3. Create a user named user1 to create and augment profiles.
Read the documentation for your operating system for information on how to create users.
4. Add the installer and user1 to the profilers group.
5. **Linux** **HP-UX** **Solaris** **AIX** Log off and log back on again as the installer to use the new group.

6. Create the following directories as the installer, if no profile was previously created:

- **Linux** **HP-UX** **Solaris** **AIX** Create the `app_server_root/logs/manageprofiles` directory:

```
mkdir app_server_root/logs/manageprofiles
```

Windows Create the `app_server_root\logs\manageprofiles` directory by following instructions in the Windows documentation. For this example procedure the directory is:

```
app_server_root\logs\manageprofiles
```

- **Linux** **HP-UX** **Solaris** **AIX** Create the `app_server_root/properties/fsdb` directory:

```
mkdir app_server_root/properties/fsdb
```

Windows Create the `app_server_root\properties\fsdb` directory by following instructions in the Windows documentation. For this example procedure the directory is:

```
app_server_root\properties\fsdb
```

7. As the installer, create the `profileRegistry.xml` file and add the appropriate information, if no profile was previously created.

Follow directions for your operating system to create the `profileRegistry.xml` file. For this example, the file paths are: **Linux** **HP-UX** **Solaris**

AIX
`app_server_root/properties/profileRegistry.xml`

Windows
`app_server_root\properties\profileRegistry.xml`

Follow instructions for your operating system to add the following information to the `profileRegistry.xml` file. The file must be encoded as UTF-8.

```
<?xml version="1.0" encoding="UTF-8"?>  
<profiles/>
```

8. As the installer, use operating system tools to change directory and file permissions.

Linux **HP-UX** **Solaris** **AIX** The following example assumes that the installation root directory is `/opt/IBM/WebSphere/AppServer`:

```

chgrp profilers /opt/IBM/WebSphere/AppServer/logs/manageprofiles
chmod g+wr /opt/IBM/WebSphere/AppServer/logs/manageprofiles
chgrp profilers /opt/IBM/WebSphere/AppServer/properties
chmod g+wr /opt/IBM/WebSphere/AppServer/properties
chgrp profilers /opt/IBM/WebSphere/AppServer/properties/fsdb
chmod g+wr /opt/IBM/WebSphere/AppServer/properties/fsdb
chgrp profilers /opt/IBM/WebSphere/AppServer/properties/profileRegistry.xml
chmod g+wr /opt/IBM/WebSphere/AppServer/properties/profileRegistry.xml
chgrp -R profilers /opt/IBM/WebSphere/AppServer/profileTemplates

```

HP-UX If you create a cell profile, additionally issue the following commands:

```

chmod -R g+wr /opt/IBM/WebSphere/AppServer/profileTemplates/cell/default/documents
chmod -R g+wr /opt/IBM/WebSphere/AppServer/profileTemplates/cell/dmgr/documents

```

HP-UX If you create an application server profile, a deployment manager profile, or a custom profile, then additionally issue the following command:

```

chmod -R g+wr /opt/IBM/WebSphere/AppServer/profileTemplates/profile_template_name/documents

```

profile_template_name is default, dmgr, or managed, respectively.

HP-UX The ownership of files is preserved when the files are copied to the profile directory during profile creation. You granted write permission to the profile directory so that files copied to the profile directory can be modified as part of the profile creation process. Files that are already in the profileTemplate directory structure prior to the start of profile creation are not modified during profile creation. **Linux**

```

chgrp profilers /opt/IBM/WebSphere/AppServer/properties/Profiles.menu
chmod g+wr /opt/IBM/WebSphere/AppServer/properties/Profiles.menu

```

Windows The following example assumes that the installation root directory is C:\Program Files\IBM\WebSphere\AppServer. Follow instructions in the Windows documentation to give the profilers group read and write permission to the following directories and their files:

```

C:\Program Files\IBM\WebSphere\AppServer\logs\manageprofiles
C:\Program Files\IBM\WebSphere\AppServer\properties
C:\Program Files\IBM\WebSphere\AppServer\properties\fsdb
C:\Program Files\IBM\WebSphere\AppServer\properties\profileRegistry.xml

```

You might have to change the permissions on additional files if the non-root user encounters permission errors. For example, if you authorize a non-root user to delete a profile, then the user might have to delete the following file:

Linux **HP-UX** **Solaris** **AIX** *app_server_root*/properties/profileRegistry.xml_LOCK

Windows *app_server_root*\properties\profileRegistry.xml_LOCK

- Give write access to the non-root user for the file to authorize the user to delete the file. If the non-root user still cannot delete the profile, then the installer can delete the profile.

Results

The installer created the profilers group and gave the group proper permissions to certain directories and files to create and augment profiles. These directories and files are the only ones in the installation root of WebSphere Application Server to which a non-root user needs to write to create and augment profiles.

What to do next

The non-root user that belongs to the profilers group can create profiles, or create and augment profiles, in a directory that the non-root user owns and to which the

non-root user has write permission. However, the non-root user cannot create profiles in the installation root directory of the product.

A non-root user ID can manage multiple profiles. The same non-root user ID can manage an entire profile, whether it is the deployment manager profile, a profile that contains the application servers and the node agent, or a custom profile. A different user ID can be used for each profile in a cell, whether global security or administrative security is enabled or disabled. The user IDs can be a mix of root and non-root user IDs. For example, the root user might manage the deployment manager profile, while a non-root user might manage a profile that contains application servers and the node agent, or vice versa. However, typically, a root user or a non-root user can manage all profiles in a cell.

The non-root user can use the same tasks to manage a profile that the root user uses.

Changing ownership for profile maintenance

When an installer installs a maintenance package that contains service for a profile that a non-root user owns, the installer owns any new files that the maintenance package creates. The installer can change the ownership of the new files so that a non-root user can successfully start the product.

Before you begin

This task assumes a basic familiarity with the Update Installer wizard and system commands.

This task uses the following terms:

- *Root users* refers to:
 - Linux HP-UX Solaris AIX Root users
 - Windows Administrators
- *Non-root users* refers to:
 - Linux HP-UX Solaris AIX Non-root users
 - Windows Non-administrators
- *Installer* refers to a root user or a non-root user.

Before you can update a profile, you must install WebSphere Application Server and create a profile. You might additionally have to augment a profile before you update it if the feature pack requires the profile to be augmented for you to use the feature-pack capabilities.

About this task

This example assumes that the installer completes the following actions:

- Applies service that creates new files in a profiles directory that the wsdemo non-root user owns
- Changes ownership of new profile files from the installer to the wsdemo non-root user.

If the installer does not change ownership, then when the non-root user starts the product, the application server encounters an error and issues a message that is similar to the following example:

ADMR0104E:

The system is unable to read document
cells/express1Cell/nodes/express1/node-metadata.properties:
java.io.IOException: No such file or directory

1. Run the update installer wizard to install maintenance packages for the product.
2. Reassign ownership of the entire profile directory to the wsdemo non-root user.

The *profile_root* variable in the following examples is the profile directory that the non-root user owns.

Linux **HP-UX** **Solaris** **AIX** Issue the **chown** command.
chown -R wsdemo *profile_root*

Windows Follow instructions in the Windows documentation to reassign ownership of the *profile_root* directory to the wsdemo non-root user.

Results

The installer installed a maintenance package that creates new files in a non-root user profile directory and changes ownership of the new files to the non-root owner.

What to do next

The non-root user can start the product without receiving the ADMR0104E error message.

Deleting profiles

You can delete a profile using the `manageprofiles` command. If the command fails, you can delete the profile using operating system commands.

Before you begin

If a node within a profile is federated to a deployment manager, before you delete the profile, stop the node and remove the node from the deployment manager. Otherwise, an orphan node is left in the deployment manager.

If you delete a profile that has augmenting templates registered to it in the profile registry, unaugment actions are attempted prior to the deletion.

You cannot delete a profile using the Profile Management Tool.

About this task

The following example attempts to delete a profile using the `manageprofiles` command, and then using operating system commands.

1. Issue the `manageprofiles` command to delete a profile.

Substitute your profile name for the *profile_name* value in the following commands.

Linux **HP-UX** **Solaris** **AIX**
./manageprofiles.sh -delete
-profileName *profile_name*

Windows
manageprofiles.bat -delete
-profileName *profile_name*

i5/OS

```
./manageprofiles -delete  
-profileName profile_name
```

If the command is successful, you have completed the task and can skip the remaining steps. If the command is partially successful or unsuccessful, proceed to the next step to delete the profile manually. If you receive the `INSTCONFFAILED: Cannot delete profile.` message, the command was unsuccessful. If the deletion is partially successful, you could receive message information similar to the following wording:

```
INSTCONFPARTIALSUCCESS: The profiles no longer exist, but errors occurred.  
For more information, consult  
app_server_root/logs/manageprofiles/deleteAll.log.
```

Distributed platforms or

The current user does not have sufficient permissions to detect or remove services. If a service does exist, then an administrative or root user has to remove it. If a service does not exist, then no further action is required.

2. Issue operating system commands to delete the profile directory.
3. Issue the following command to remove references in the registry to deleted profiles:

Linux

HP-UX

Solaris

AIX

```
./manageprofiles.sh -validateAndUpdateRegistry
```

Windows

```
manageprofiles.bat -validateAndUpdateRegistry
```

i5/OS

```
manageprofiles -validateAndUpdateRegistry
```

Editing of the registry is not recommended.

Results

You have now deleted a profile.

What to do next

i5/OS You can delete other profiles using this procedure, or create other profiles using the `manageprofiles` command.

Distributed platforms You can delete other profiles using this procedure, or create other profiles using the `manageprofiles` command or the Profile Management Tool.

Chapter 6. Directory conventions

References in product information to *app_server_root*, *profile_root*, and other directories infer specific default directory locations. This topic describes the conventions in use for WebSphere Application Server.

z/OS

Default product locations - z/OS

app_server_root

Refers to the top directory for a WebSphere Application Server node.

The node may be of any type—application server, deployment manager, or unmanaged for example. Each node has its own *app_server_root*. Corresponding product variables are `was.install.root` and `WAS_HOME`.

The default varies based on node type. Common defaults are *configuration_root*/AppServer and *configuration_root*/DeploymentManager.

configuration_root

Refers to the mount point for the configuration file system (formerly, the configuration HFS) in WebSphere Application Server for z/OS.

The *configuration_root* contains the various *app_server_root* directories and certain symbolic links associated with them. Each different node type under the *configuration_root* requires its own cataloged procedures under z/OS.

The default is `/wasv7config/cell_name/node_name`.

plug-ins_root

Refers to the installation root directory for Web Server plug-ins.

profile_root

Refers to the home directory for a particular instantiated WebSphere Application Server profile.

Corresponding product variables are `server.root` and `user.install.root`.

In general, this is the same as *app_server_root*/profiles/*profile_name*. On z/OS, this will be always be *app_server_root*/profiles/default because only the profile name "default" is used in WebSphere Application Server for z/OS.

smpe_root

Refers to the root directory for product code installed with SMP/E.

The corresponding product variable is `smpe.install.root`.

The default is `/usr/lpp/zWebSphere/V7R0`.

i5/OS

Default product locations - IBM i

These file paths are default locations. You can install the product and other components in any directory where you have write access. You can create profiles in any valid directory where you have write access. Multiple installations of WebSphere Application Server products or components require multiple locations.

app_client_root

The default installation root directory for the Java EE WebSphere Application Client is the /QIBM/ProdData/WebSphere/AppClient/V7/client directory.

app_client_user_data_root

The default Java EE WebSphere Application Client user data root is the /QIBM/UserData/WebSphere/AppClient/V7/client directory.

app_client_profile_root

The default Java EE WebSphere Application Client profile root is the /QIBM/UserData/WebSphere/AppClient/V7/client/profiles/*profile_name* directory.

app_server_root

The default installation root directory for WebSphere Application Server Network Deployment is the /QIBM/ProdData/WebSphere/AppServer/V7/ND/QIBM/ProdData/WebSphere/AppServer/V7/*product* directory.

cip_app_server_root

The default installation root directory is the /QIBM/ProdData/WebSphere/AppServer/V7/ND/QIBM/ProdData/WebSphere/AppServer/V7/*product* directory for a customized installation package (CIP) produced by the Installation Factory.

A CIP is a WebSphere Application Server Network Deployment product bundled with optional maintenance packages, an optional configuration archive, one or more optional enterprise archive files, and other optional files and scripts.

cip_profile_root

The default profile root directory is the /QIBM/UserData/WebSphere/AppServer/V7/ND/cip/*cip_uid*/profiles/*profile_name*/QIBM/UserData/WebSphere/AppServer/V7/*product*/cip/*cip_uid*/profiles/*profile_name* directory for a customized installation package (CIP) produced by the Installation Factory.

cip_user_data_root

The default user data root directory is the /QIBM/UserData/WebSphere/AppServer/V7/ND/cip/*cip_uid*/QIBM/UserData/WebSphere/AppServer/V7/*product*/cip/*cip_uid* directory for a customized installation package (CIP) produced by the Installation Factory.

if_root

This directory represents the root directory of the IBM WebSphere Installation Factory. Because you can download and unpack the Installation Factory to any directory on the file system to which you have write access, this directory's location varies by user. The Installation Factory is an Eclipse-based tool which creates installation packages for installing WebSphere Application Server in a reliable and repeatable way, tailored to your specific needs.

iip_root

This directory represents the root directory of an *integrated installation package* (IIP) produced by the IBM WebSphere Installation Factory. Because you can create and save an IIP to any directory on the file system to which you have write access, this directory's location varies by user. An IIP is an aggregated installation package created with the Installation Factory that can include one or more generally available installation packages, one or more customized installation packages (CIPs), and other user-specified files and directories.

java_home

Table 123. Root directories for supported Java Virtual Machines.

This table shows the root directories for all supported Java Virtual Machines (JVMs).

| JVM | Directory |
|--------------------------------|--|
| Classic JVM | /QIBM/ProdData/Java400/jdk6 |
| 32-bit IBM Technology for Java | /QOpenSys/QIBM/ProdData/JavaVM/jdk60/32bit |
| 64-bit IBM Technology for Java | /QOpenSys/QIBM/ProdData/JavaVM/jdk60/64bit |

plugins_profile_root

The default Web server plug-ins profile root is the /QIBM/UserData/WebSphere/Plugins/V7/webserver/profiles/*profile_name* directory.

plugins_root

The default installation root directory for Web server plug-ins is the /QIBM/ProdData/WebSphere/Plugins/V7/webserver directory.

plugins_user_data_root

The default Web server plug-ins user data root is the /QIBM/UserData/WebSphere/Plugins/V7/webserver directory.

product_library

product_lib

This is the product library for the installed product. The product library for each Version 7.0 installation on the system contains the program and service program objects (similar to .exe, .dll, .so objects) for the installed product. The product library name is QWAS7x (where x is A, B, C, and so on). The product library for the first WebSphere Application Server Version 7.0 product installed on the system is QWAS7A. The *app_server_root/properties/product.properties* file contains the value for the product library of the installation, was.install.library, and is located under the *app_server_root* directory.

profile_root

The default directory for a profile named *profile_name* for WebSphere Application Server Network Deployment is the /QIBM/UserData/WebSphere/AppServer/V7/ND/profiles/*profile_name*/QIBM/UserData/WebSphere/AppServer/V7/product/profiles/*profile_name* directory.

shared_product_library

The shared product library, which contains all of the objects shared by all installations on the system, is QWAS7. This library contains objects such as the product definition, the subsystem description, the job description, and the job queue.

updi_root

The default installation root directory for the Update Installer for WebSphere Software is the /QIBM/ProdData/WebSphere/UpdateInstaller/V7/updi directory.

user_data_root

The default user data directory for WebSphere Application Server Network Deployment is the /QIBM/UserData/WebSphere/AppServer/V7/ND/QIBM/UserData/WebSphere/AppServer/V7/product directory.

The profiles and profileRegistry subdirectories are created under this directory when you install the product.

web_server_root

The default web server path is /www/*web_server_name*.

Default product locations (distributed)

The following file paths are default locations. You can install the product and other components or create profiles in any directory where you have write access. Multiple installations of WebSphere Application Server Network Deployment products or components require multiple locations. Default values for installation actions by root and non-root users are given. If no non-root values are specified, then the default directory values are applicable to both root and non-root users.

app_client_root

Table 124. Default installation root directories for the WebSphere Application Client.

This table shows the default installation root directories for the WebSphere Application Client.

| User | Directory |
|----------|--|
| Root | <p>AIX /usr/IBM/WebSphere/AppClient (Java EE Application client only)</p> <p>HP-UX Linux Solaris /opt/IBM/WebSphere/AppClient (Java EE Application client only)</p> <p>Windows C:\Program Files\IBM\WebSphere\AppClient</p> |
| Non-root | <p>AIX HP-UX Linux Solaris <i>user_home</i>/IBM/WebSphere/AppClient (Java EE Application client only)</p> <p>Windows C:\IBM\WebSphere\AppClient</p> |

app_server_root

Table 125. Default installation directories for WebSphere Application Server.

This table shows the default installation directories for WebSphere Application Server Network Deployment.

| User | Directory |
|----------|--|
| Root | <p>AIX /usr/IBM/WebSphere/AppServer</p> <p>HP-UX Linux Solaris /opt/IBM/WebSphere/AppServer</p> <p>Windows C:\Program Files\IBM\WebSphere\AppServer</p> |
| Non-root | <p>AIX HP-UX Linux Solaris <i>user_home</i>/IBM/WebSphere/AppServer</p> <p>Windows C:\IBM\WebSphere\AppServer</p> |

cip_app_server_root

A *customized installation package* (CIP) is an installation package created with IBM WebSphere Installation Factory that contains a WebSphere Application Server or feature pack product bundled with one or more maintenance packages, an optional configuration archive, one or more optional enterprise archive files, and other optional files and scripts.

Table 126. Default installation root directories for a CIP.

This table shows the default installation root directories for a CIP.

| User | Directory |
|----------|--|
| Root | AIX /usr/IBM/WebSphere/AppServer |
| | HP-UX Linux Solaris /opt/IBM/WebSphere/AppServer |
| | Windows C:\Program Files\IBM\WebSphere\ AppServer |
| Non-root | AIX HP-UX Linux Solaris user_home/IBM/WebSphere/AppServer |
| | Windows C:\IBM\WebSphere\AppData |

component_root

The component installation root directory is any installation root directory described in this topic. Some programs are for use across multiple components. In particular, the Update Installer for WebSphere Software is for use with WebSphere Application Server Network Deployment, Web server plug-ins, the Application Client, and the IBM HTTP Server. All of these components are part of the product package.

gskit_root

IBM Global Security Kit (GSKit) can now be installed by any user. GSKit is installed locally inside the installing product's directory structure and is no longer installed in a global location on the target system. The following list shows the default installation root directory for Version 7 of the GSKit, where *product_root* is the root directory of the product that is installing GSKit, for example IBM HTTP Server or the Web server plug-in.

AIX **HP-UX** **Linux** **Solaris**
product_root/gsk7

Windows
product_root\gsk7

if_root This directory represents the root directory of the IBM WebSphere Installation Factory. Because you can download and unpack the Installation Factory to any directory on the file system to which you have write access, this directory's location varies by user. IBM WebSphere Installation Factory is an Eclipse-based tool which creates installation packages for installing WebSphere Application Server in a reliable and repeatable way, tailored to your specific needs.

iip_root

This directory represents the root directory of an *integrated installation package* (IIP) produced by the IBM WebSphere Installation Factory. Because you can create and save an IIP to any directory on the file system to which you have write access, this directory's location varies by user. An IIP is an aggregated installation package that can include one or more generally available installation packages, one or more customized installation packages (CIPs), and other user-specified files and directories.

profile_root

Table 127. Default profile directories.

This table shows the default directories for a profile named *profile_name* on each distributed operating system.

| User | Directory |
|----------|---|
| Root | AIX /usr/IBM/WebSphere/AppServer/profiles/ <i>profile_name</i> HP-UX Linux Solaris /opt/IBM/WebSphere/AppServer/profiles/ <i>profile_name</i> Windows C:\Program Files\IBM\WebSphere\AppServer\profiles\ <i>profile_name</i> |
| Non-root | AIX HP-UX Linux Solaris <i>user_home</i> /IBM/WebSphere/AppServer/profiles/ Windows C:\IBM\WebSphere\AppServer\profiles\ |

plugins_root

Table 128. Default installation root directories for the Web server plug-ins.

This table shows the default installation root directories for the Web server plug-ins for WebSphere Application Server.

| User | Directory |
|----------|---|
| Root | AIX /usr/IBM/WebSphere/Plugins HP-UX Linux Solaris /opt/IBM/WebSphere/Plugins Windows C:\Program Files\IBM\WebSphere\Plugins |
| Non-root | AIX HP-UX Linux Solaris <i>user_home</i> /IBM/WebSphere/Plugins Windows C:\IBM\WebSphere\Plugins |

Note: If the Web server plug-ins are installed as part of the IBM HTTP Server installation, the installation location is inside the IBM HTTP Server installation location. For example:

/opt/IBM/HTTPServer/Plugins

updi_root

Table 129. Default installation root directories for the Update Installer for WebSphere Software.

This table shows the default installation root directories for the Update Installer for WebSphere Software.

| User | Directory |
|----------|--|
| Root | AIX /usr/IBM/WebSphere/UpdateInstaller HP-UX Linux Solaris /opt/IBM/WebSphere/UpdateInstaller Windows C:\Program Files\IBM\WebSphere\UpdateInstaller |
| Non-root | AIX HP-UX Linux Solaris user_home/IBM/WebSphere/UpdateInstaller Windows C:\IBM\WebSphere\UpdateInstaller |

web_server_root

Table 130. Default installation root directories for the IBM HTTP Server.

This table shows the default installation root directories for the IBM HTTP Server.

| User | Directory |
|----------|---|
| Root | AIX /usr/IBM/HTTPServer HP-UX Linux Solaris /opt/IBM/HTTPServer Windows C:\Program Files\IBM\HTTPServer |
| Non-root | AIX HP-UX Linux Solaris user_home/IBM/HTTPServer Windows C:\IBM\HTTPServer |

Appendix A. Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, is the user's responsibility.

IBM may have patents or pending patent applications covering subject matter 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 the following address:

IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, New York 10594
USA

Appendix B. Trademarks and service marks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ([®] or [™]), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. For a current list of IBM trademarks, visit the IBM Copyright and trademark information Web site (www.ibm.com/legal/copytrade.shtml).

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java is a trademark of Sun Microsystems, Inc. in the United States, other countries, or both.

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