WebSphere® Application Server for z/OS, Version 7.0

Installing your application serving environment

GA32-0601-00

Note

Before using this information, be sure to read the general information under “Notices” on page 397.

Compilation date: September 23, 2008

Contents

How to send your comments

Your feedback is important in helping to provide the most accurate and highest quality information.

- To send comments on articles in the WebSphere Application Server Information Center
  1. Display the article in your Web browser and scroll to the end of the article.
  2. Click on the **Feedback** link at the bottom of the article, and a separate window containing an e-mail form appears.
  3. Fill out the e-mail form as instructed, and click on **Submit feedback** .
- To send comments on PDF books, you can e-mail your comments to: **wasdoc@us.ibm.com** or fax them to 919-254-5250.

  Be sure to include the document name and number, the WebSphere Application Server version you are using, and, if applicable, the specific page, table, or figure number on which you are commenting.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Changes to serve you more quickly

Print sections directly from the information center navigation

PDF books are provided as a convenience format for easy printing, reading, and offline use. The information center is the official delivery format for IBM WebSphere Application Server documentation. If you use the PDF books primarily for convenient printing, it is now easier to print various parts of the information center as needed, quickly and directly from the information center navigation tree.

To print a section of the information center navigation:

1. Hover your cursor over an entry in the information center navigation until the **Open Quick Menu** icon is displayed beside the entry.
2. Right-click the icon to display a menu for printing or searching your selected section of the navigation tree.
3. If you select **Print this topic and subtopics** from the menu, the selected section is launched in a separate browser window as one HTML file. The HTML file includes each of the topics in the section, with a table of contents at the top.
4. Print the HTML file.

For performance reasons, the number of topics you can print at one time is limited. You are notified if your selection contains too many topics. If the current limit is too restrictive, use the feedback link to suggest a preferable limit. The feedback link is available at the end of most information center pages.

Under construction!

The Information Development Team for IBM WebSphere Application Server is changing its PDF book delivery strategy to respond better to user needs. The intention is to deliver the content to you in PDF format more frequently. During a temporary transition phase, you might experience broken links. During the transition phase, expect the following link behavior:

- Links to Web addresses beginning with http:// work
- Links that refer to specific page numbers within the same PDF book work
- The remaining links will *not* work. You receive an error message when you click them

Thanks for your patience, in the short term, to facilitate the transition to more frequent PDF book updates.

Chapter 1. What is new for installers

Installation is now easier, more consistent, and a more functionally rich experience across platforms, installable components, and types of installations.

- Installing maintenance packages

  The V7.0 Update Installer supports multiple releases. The V7.0 Update Installer is also compatible with earlier releases; it works with V6.0.2.21 and newer maintenance and any maintenance for V6.1.0.x and V7.0 releases. This allows a single instance of the Update Installer to apply maintenance to more than one version of the application server. For V6.0.2.19 and previous releases, apply maintenance with the V6.0.2.x Update Installer.

  The Update Installer has a file permission verification feature. This feature saves time and allows you to resolve potential file permission problems for Application Server maintenance before you install it.

  The Update Installer can update language packs to add new languages. The Update Installer supports updates for DMZ Secure Proxy Server.

  The Update Installer is available in .tar format on Unix type operating systems.

  When installing the Update Installer, you can choose to create or not create start menu shortcuts.
- “Configuring z/OS application-serving environments with the Profile Management Tool” on page 285

  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 profiles and upload the associated jobs and instructions to the target z/OS system.
- “Configuring z/OS application-serving environments with the zpmt command” on page 301

  The **zpmt** command is an alternative to the Profile Management Tool 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.
- “Target system requirements” on page 10

  WebSphere Customization Tools Version 7.0 is an Eclipse-based tool that contains the Profile Management Tool (z/OS only) and the z/OS Migration Management Tool for Version 7.0.

Chapter 2. How do I install an application serving environment?

Follow these shortcuts to get started quickly with popular tasks.

When you visit a task in the information center, look for the **IBM Suggests** feature at the bottom of the page. Use it to find available tutorials, demonstrations, presentations, developerWorks® articles, Redbooks®, support documents, and more.

Review the software and hardware prerequisites

Plan your installation

Prepare the base operating system

Install the product and additional software

Plan for product configuration

Configure the product

Apply product maintenance

Troubleshoot installation and configuration

Chapter 3. Installing a DMZ Secure Proxy Server for IBM WebSphere Application Server

Use this topic to install a DMZ Secure Proxy Server for IBM® WebSphere® Application Server using the launchpad. Installing the DMZ Secure Proxy Server for IBM WebSphere Application Server allows a secure proxy server profile to be created outside of the cell.

About this task

Complete the following steps to install a DMZ Secure Proxy Server for IBM WebSphere Application Server.

1. Prepare your operating system for installing DMZ Secure Proxy Server for IBM WebSphere Application Server as you would for installing any of the installable components on the product disc. Refer to the Information center topic *Preparing the operating system for product installation*.
2. Insert the product disc and mount the disc if necessary.
3. Start the installation with the following launchpad command:

   You can also start the installation from the secure_proxy directory, where secure_proxy is the installable component directory on the product disc. Launch the following command from the product disc:
4. The installation wizard initializes and then displays the Welcome panel.

   Click **Next** to continue.
5. The license agreement panel is displayed. Read the license agreement and accept its terms. After you accept the licensing terms, the installation wizard checks for a supported operating system and prerequisite patches.

   Although the installation wizard automatically checks for prerequisite operating system patches with the prereqChecker application, review the prerequisites on the WebSphere Application Server detailed system requirements Web site if you have not already done so. The Web site lists all supported operating systems and the operating system fixes and patches that you must install to have a compliant operating system.

   The installation process verifies that the minimum required version of a supported operating system is available. If you meet the minimum release requirements or are at a higher *minor* release of a supported operating system, then you will not encounter a prerequisite error. If you are not at the minimum version of a supported operating system, you can continue with the installation, but the installation or product operation might not succeed without applying maintenance. If you are at a higher *major* release of a supported operating system, or the operating system itself is not on the supported list, you might encounter the following warning:

   ```
   Warning: A supported operating system was not detected.

   Support for your operating system might have been added after the release of the product.
   See the WebSphere Application Server detailed system requirements Web pages for more information
   about supported operating systems. You can continue with the installation, but the installation
   or product operation might not succeed without applying maintenance. Go to the product support Web pages
   to obtain the latest maintenance packages to apply after installation.
   ```

   Refer to the documentation for non-IBM prerequisite and corequisite products to learn how to migrate to their supported versions.

   Click the radio button beside the message **I accept both the IBM and the non-IBM terms** to agree to the license agreement and click **Next** to continue.
6. The systems prerequisite check panel is displayed. After confirming that your operating system is supported and that you have installed all necessary patches, click **Next** to continue. The Installation wizard checks for a previous application server installation at the same product level.
7. If you are installing the product as a non-root user (or a non Administrator on Windows operating systems), then a panel is displayed indicating that a non-root user has been detected. This panel contains important information about installing as a non-root user. Click **Next**.

8. If the wizard detects a previous installation, then the product detection panel is displayed. If the wizard does not detect a previous installation, then skip this step.

   You have the following options:

   - Install a new copy of the IBM WebSphere Application Server Network Deployment.
   - Create a new WebSphere Application Server profile using the Profile Management Tool.

   This procedure assumes that you do not have an existing installation that you intend to update.
9. The installation directory panel is displayed. Specify the destination of the installation root directory and click **Next**.

   Specify the location of the installation root directory for the product binaries, which are also known as the core product files or system files.

   The core product files do not change unless you:

   - Add a feature
   - Install maintenance, such as refresh packs, fix packs, or interim fixes
   - Install another product that extends the Network Deployment product.

   The system-owned default *app_server_root* directories for installing as a root user or an administrator are different than the user-owned default *app_server_root* directories when installing as a non-root installer.

   Note:

   - Deleting the default target location and leaving an installation directory field empty prevents you from continuing.

   The installer program checks for required space before calling the Installation wizard. If you do not have enough space, stop the installation program, free space by deleting unused files and emptying the recycle bin, then restart the installation.
10. Select an initial server environment on the WebSphere Application Server environments panel.

    The following values are valid:

Table 1. Profile types

Profile Type	Description
Management	Create a management profile that provides the servers and services necessary to manage your WebSphere environment. A management profile includes an administrative agent server and services for managing multiple application server environments. An administrative agent manages application servers that are on the same workstation.
Secure proxy	Create a secure proxy server to take requests from the internet and forward them to application servers. The secure proxy server resides in the DMZ.
None	Do not create a profile during installation. However, if you do not create a profile during installation, then you must create a profile after installation to have an operational product.

11. The administrative security panel is displayed. Choose whether to enable administrative security and click **Next.** The default setting is to enable administrative security. Clear the check box to disable security or supply an administrative ID and password.
12. The installation summary panel is displayed.

    Review the summary information. Click **Next** to install the product code or **Back** to change your specifications.

    The installation wizard creates the uninstaller program and then displays a progress panel that shows which components are being installed.
13. The Installation results panel is displayed. Verify the success of the installer program by examining the completion panel and the *app_server_root*/logs/install/log.txt file to verify that there were no file

system or other unusual errors while installing. If there are problems, correct them, and reinstall the product. Important information about the profile you created is also available in *profile_root*/logs/AboutThisProfile.txt. See for more information on other installation logs and log locations.

If the installation of the core product files fails, fix the error and reinstall.

Read the and topics for more information.

If problems exist that cause you to reinstall the product, correct the errors, uninstall the product as described in , reboot a Windows machine or log off and back on as root on a machine with an operating system such as AIX or Linux, and reinstall.

14. Click **Finish** to close the installation wizard.

    If you did not create a profile during the installation, the option to launch the Profile Management Tool is displayed. Use the Profile Management Tool to create an operational environment that includes a profile.

    If you did create a profile, select the check box to open the First Steps console then click **Finish**.

Results

The installation wizard installs the product files into the installation root directory.

Uninstalling a DMZ Secure Proxy Server for IBM WebSphere Application Server

Use this topic to uninstall a DMZ Secure Proxy Server for IBM WebSphere Application Server using the launchpad.

Before you begin

The uninstaller program created during installation removes registry entries, uninstalls the server, and removes all related features. The uninstaller program does not remove log files in the installation root directory. The uninstaller program is launched by the uninstall command.

Note: The uninstaller is able to detect other products that extend the secure proxy server and have a dependency on the server. If you have installed other products that extend the server, you must uninstall those products before uninstalling the secure proxy server. Products that extend the server are feature packs and other products that rely on the server runtime environment.

About this task

The time required to uninstall the DMZ Secure Proxy Server for IBM WebSphere Application Server depends on the processing speed of your machine. As a guideline, uninstalling the core product files and one profile takes approximately 10 minutes when using the uninstall command.

Complete the following steps to uninstall a DMZ Secure Proxy Server for IBM WebSphere Application Server.

1. Log on using the same user ID that was used when the product was installed.
2. **Optional:** Back up configuration files and log files to refer to them later if necessary. The uninstaller program removes all profiles by default, including all of the configuration data and applications in each profile.

   Use the AdminTask command scripting interface to create a configuration archive file of an existing profile, for example. You can back up the config folder and the logs folder of each profile; however, the secure proxy server cannot reuse profiles; therefore, you are not required to back up an entire profile.
3. Issue the uninstall command from the directory where the server is installed. Refer to the information topic on directory conventions, if needed:

   The uninstaller wizard begins and displays the Welcome panel.

4. 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.

   a. Click **Next** to continue uninstalling the product.

      When using the wizard, a panel allows you to choose whether or not the uninstaller deletes all profiles before it deletes the core product files. By default, all profiles are deleted, but this option can be deselected on the panel.

      To change the default behavior, start the wizard with this command:

      ```
      uninstall -OPT removeProfilesOnUninstall="false"
      ```

      After uninstalling profiles, the uninstaller program deletes the core product files in component order.

   b. Click **Finish** to close the wizard after the wizard removes the product.

5. Review the log file.

   The log file records file system or other unusual errors. Look for the INSTCONFSUCCESS indicator of success in the log:

   ```
   (date_time),
   Uninstall, com.ibm.ws.install.ni.ismp.actions.
   SetExitCodeAction, msg1,
   CWUPI0000I: EXITCODE=0
   (date_time),
   Uninstall, com.ibm.ws.install.ni.ismp.actions.
   ISMPLogSuccessMessageAction, msg1,
   INSTCONFSUCCESS
   ```

6. If any product files remain, uninstall those files manually before reinstalling the secure proxy server.

Results

This procedure results in uninstalling the DMZ Secure Proxy Server for IBM WebSphere Application Server.

Chapter 4. Task overview: Installing

This article describes the process of installing and configuring WebSphere Application Server for z/OS®.

Before you begin

This article introduces the context of installing and customizing IBM WebSphere Application Server for z/OS, including the tasks you need to perform before and after installing. The product is provided in both U.S. English and Japanese.

To create a complete, customized WebSphere Application Server for z/OS application serving environment, you need to install the product code, prepare the z/OS operating system and subsystems, run the Profile Management Tool or zpmt command, follow the customized instructions and run the generated jobs, and bring up your servers.

Note: See “Building a practice WebSphere Application Server for z/OS cell” on page 84 for steps you can follow to set up a practice version of WebSphere Application Server for z/OS if you want to just get the feel for it or see the basics.

About this task

Perform the following tasks to create a running version of the product on your machine.

1. Plan dataset names and layout for product code installation as described in Chapter 5, “Planning for installation,” on page 29.
2. Install WebSphere Application Server for z/OS as described in Chapter 6, “Installing the product and additional software,” on page 35. You must first load the WebSphere Application Server for z/OS code onto your system using SMP/E or a preloaded product offering before you make it usable through customization.
3. Prepare your z/OS target systems to run WebSphere Application Server for z/OS as described in Chapter 7, “Preparing the base operating system,” on page 39.
4. Choose your application serving environment and decide on its initial characteristics as described in Chapter 8, “Planning for product configuration,” on page 49.
5. Configure WebSphere Application Server for z/OS as described in Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 285. Once you have the WebSphere Application Server for z/OS code installed on your system, you are ready to make it your own by customizing it.
6. To create additional application serving environments, repeat the steps in Chapter 8, “Planning for product configuration,” on page 49 and Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 285.
7. Tune for performance.

Results

You are ready to deploy and run applications using the WebSphere Application Server for z/OS product.

Hardware and software requirements on z/OS

This topic describes hardware and software prerequisites for installing WebSphere Application Server for z/OS.

See the Supported hardware and software Web page for the complete up-to-date listings on what is supported.

If there is a conflict between the information provided in the information center and the information on the Supported hardware and software pages, the information at the Web site takes precedence. Prerequisites information in the information center is provided as a convenience only.

WebSphere Application Server for z/OS Version 7 requires z/OS or z/OS.e Version 1 Release 7 and runs on any hardware that supports the required operating system software.

For detailed hardware and software requirements for installing WebSphere Application Server for z/OS, see “Driving system requirements.”

For detailed hardware and software requirements for customizing and running WebSphere Application Server for z/OS application serving environments, see “Target system requirements.”

Driving system requirements

This article describes prerequisites for installing WebSphere Application Server for z/OS.

Hardware requirements

Go to the WebSphere Application Server detailed system requirements Web page for up-to-date listings on what hardware is required.

The hardware requirements for this product are any hardware that supports z/OS Version 1 Release 7 or later. However, there are significant performance advantages for those applications doing floating point arithmetic if the machine has binary floating point hardware, such as S/390® Parallel Enterprise Server-Generation 5 and later systems.

You should plan on three 3390-3 DASD volumes (or equivalent storage) for the product target and distribution libraries and the product HFS, and an additional 3390-3 DASD volume (or equivalent storage) for CustomPac dialogs and work datasets (if you install using a ServerPac or SystemPac®) or for SMP/E work datasets and relfile storage (if you install using a Custom-Build Product Delivery Offering).

Software requirements

Go to the WebSphere Application Server detailed system requirements Web page for up-to-date listings on what software is required.

The z/OS system used to install WebSphere Application Server for z/OS must run z/OS UNIX® System Services (z/OS UNIX) with an HFS or ZFS file system configured. For details, see *z/OS UNIX System Services Planning*.

You must have IBM Software Development Kit (SDK) for z/OS, Java™ 2 Technology Edition Version 1.4 or above or another Java SDK (level 1.4 or above). This is required to provide the jar command used during SMP/E APPLY or RESTORE processing.

Consult the Program Directory and PSP bucket for any additional required corrective service.

Target system requirements

Prerequisites for configuring and running WebSphere Application Server for z/OS application serving environments are listed below.

Hardware requirements

The hardware requirements for this product are any hardware that supports z/OS Version 1 Release 7 or later. However, there are significant performance advantages for those applications doing floating point arithmetic if the machine has binary floating point hardware, such as S/390 Parallel Enterprise Server-Generation 5 and later systems.

The LPAR in which the WebSphere Application Server for z/OS runtime and initial application servers run requires a minimum of 512 MB of real storage. You might need to increase the real storage size depending on the size and number of application servers you deploy. In addition, you might want to increase your JES spool space if you use WebSphere Application Server for z/OS tracing options to the STDOUT DD dataset.

In addition to the DASD volumes used to hold the product code and file system, you will need additional DASD storage to hold configuration data for application serving environments. The amount of storage depends on the number of environments and the size and complexity of the applications being deployed.

WebSphere Application Server for z/OS is a heavy user of auxiliary storage. You might want to add additional paging volumes before configuring application serving environments.

WebSphere Application Server for z/OS Version 7.0 offers full support for zAAPs. zAAPs are designed to operate asynchronously with the general purpose processors when executing Java™ programming under control of the IBM JVM. The IBM JVM processing cycles can be executed on the configured zAAPS, with no anticipated modifications to the Java applications.

The zAAPs may be purchased and installed on z9™ – 109, z990 and z890 servers (and follow-on models only). In order to exploit a zAAP, the operating system level must be z/OS Version 1 Release 7 (or z/OS.e Version 1 Release 7).

IBM System z® Application Assist Processors (zAAPs) are attractively priced specialized processing units that provide a strategic z/OS Java™ execution environment for customers who desire the powerful integration advantages and traditional qualities of service of the IBM mainframe platform. zAAP can help you strategically integrate and run new Java-based Web applications with core z/OS business applications and backend database systems, increase overall system productivity, and ultimately lower the overall cost of computing for running Java technology-based workloads on the platform.

For more details, see the IBM zAAP Redbooks at http://www.redbooks.ibm.com/abstracts/sg246386.html?Open .

Software requirements

You need to enable, and configure the following z/OS elements, features, and components on each z/OS target system. Consult the WebSphere Application Server for z/OS Program Directory and PSP bucket for any additional required corrective service not listed here. In some cases, this corrective service must be installed on each target system for WebSphere Application Server to start.

All of the z/OS sources referenced are available at this Web site: http://www.ibm.com/servers/eserver/zseries/zos/bkserv/

- z/OS (or z/OS.e) Version 1 Release 7 or later, configured as a sysplex (in the case of a single z/OS system, as a monoplex). For details, see *z/OS MVS Setting Up a Sysplex*.
- z/OS UNIX System Services (z/OS UNIX) with an HFS or ZFS file system. For details, see *z/OS UNIX System Services Planning*.
- eNetwork Communications Server (TCP/IP) or equivalent. In this manual, we refer to eNetwork Communications Server; but you can substitute an equivalent product. For details, see *z/OS Communications Server: IP Migration*.

- Resource recovery services (RRS). For details, see *z/OS MVS Programming: Resource Recovery*.
- System logger. For details, see *z/OS MVS Setting up a Sysplex*.
- A security product such as z/OS Security Server (RACF®). In this manual, we refer to Security Server in examples; but you can substitute an equivalent security product. For details, see *z/OS Security Server RACF Migration*.

Additional software might be required to support particular product functions.

Table 2. Software requirements for optional functions

If you plan to use . . .	Then you need . . .	Notes . . .
WebSphere Application Server for z/OS IMS™ Connect Version 8.1 support	IMS/TM 8.1.0 or later	The connector is called IMS Connector for Java Version 2.2
WebSphere Application Server for z/OS CICS® Transaction Gateway 5.0.1 support	CICS/TS Version 2.2 or later	CTG Version 6.0 (CICS Transaction Gateway)
DB2®	DB2 Version 7.1 or later	DB2 Version 7.1 and later are supported for use with configuration options and applications which may require a database.
DB2 SQLJ in J2EE application components	DB2 Version 7.1 or later with PTFs satisfying APARs PQ84404 PQ86525 PQ89043 PQ80841 UQ88238 PQ88082 PQ87786 PQ88082 UQ86911 PQ51847 – DB2 Version 8.1 or later with PTFs satisfying APARs PK00615 PQ84577 PQ87786 PQ88082 UQ86912	DB2 Version 7.1 and later are supported for use with configuration options and applications which may require a database. DB2 Version 7.1 is no longer a prerequisite for WebSphere Application Server for z/OS, though some functions might still require it. For example, session persistence requires an existing database. Check your configuration. DB2 SQLJ in J2EE application components, DB2 Version 7.1 PTFUQ59527 DB2 is no longer a prerequisite for Websphere Application Server for z/OS, though some functions might still require it.
Connectors	WebSphere Application Server for z/OS supports any resource adapter that is designed to use the 1.0 level of the J2EE Connector Architecture (JCA). Install the listed IBM connectors if you want to access your IMS or CICS legacy data. For details on how to define and install a specific connector, see the documentation for that particular connector product.	
	For the CICS Transaction Gateway ECI connector: • CICS Transaction Gateway Version 6.0 or later • WebSphere Studio Application Developer IE Version 5.0	
	For the IMS Connector for Java: • IMS Connect for z/OS Version 2.1 • IMS Version 8 or later • WebSphere Studio Application Developer IE Version 5.0.1	
	For the IMS JDBC Connector: • IMS Version 8	

Table 2. Software requirements for optional functions (continued)

If you plan to use . . .	Then you need . . .	Notes . . .
Profile Management Tool	WebSphere Customization Tools Version 7.0 **Note:** WebSphere Customization Tools Version 7.0 is an Eclipse-based tool that contains the Profile Management Tool (z/OS only) and the z/OS Migration Management Tool for Version 7.0.	
SAF writable key rings	z/OS Version 1.9 or later, or z/OS Version 1.8 with APARs OA22287 (RACF) and OA22295 (SAF)	
Migration function	z/OS UNIX System Services APARs OA25489, OA22093 (USS), and OA22094 (MVS)	

Skill requirements

In assembling your project team, you should consider the skills you need to implement WebSphere Application Server for z/OS. This article discusses the recommended skill set necessary to support the following configurations:

- Basic configurations
- Production environments

Documentation to support the z/OS skills described in this article can be found at the following Web site: z/OS Internet Library

For basic configurations:

Below are the recommended skills necessary to support a basic configuration:

- z/OS UNIX System Services and the hierarchical file system (HFS) - to set up a functional HFS and UNIX environment
- eNetwork Communications Server (TCP/IP) or equivalent - to configure connectivity for WebSphere Application Server for z/OS clients and servers
- Resource recovery services (RRS) - to implement resource recovery services and to support two-phase commit transactions
- Security Server (RACF), or the security product you use - to authenticate WebSphere Application Server for z/OS clients and servers, and authorize access to resources
- Secure Sockets Layer (SSL) - to enable security if desired (recommended)
- SMP/E and JCL
- System logger - to set up log streams for RRS and the WebSphere Application Server for z/OS error log
- Webserver - to support HTTP clients if desired
- Workload management (WLM)
- Java and WebSphere Application Server tooling - to support application development and deployment

Depending on the needs of the applications you deploy, you might also need skills to configure the resource managers your applications require, such skills might include CICS, DB2, IMS, and MQ.

For production environments:

As you move your system toward a production environment, you need to have the following system skills available:

- Automatic restart management (ARM)
- System Automation, if you have it installed, or whichever automation you prefer to use
- Sysplex if you plan to use WebSphere Application Server for z/OS in a cell that spans systems
- Sysplex Distributor (part of eNetwork Communications Server), if you plan to create a high availability environment
- RMF™ or other performance measurement systems

Creating your implementation plan

Before you begin

We assume that you have a z/OS system on which you will implement WebSphere Application Server for z/OS.

About this task

To get started, plan to build your initial WebSphere Application Server for z/OS application serving environment servers on one system, then replicate them on other systems as you expand into a cell. This procedure first guides you through initial planning and implementation of WebSphere Application Server for z/OS on a monoplex. Then, it guides you through setting up your application development and client environments. Finally, the procedure guides you through planning for optional advanced system configurations.

Perform the following steps to implement your plan, checking off each item as you complete it:

1. Determine the skills that you need.
   See “Skill requirements” on page 13 for more information.
2. Determine WebSphere Application Server for z/OS system requirements.
   See “Hardware and software requirements on z/OS” on page 9 for more information.
3. Understand the security options, and prepare for securing your system.
4. Implement Workload Management in goal mode on each z/OS system if necessary.
   See “Workload management” on page 66 for more information.
5. Implement Resource Recovery Services (if not already implemented) on each z/OS system.
   See “Preparing Resource Recovery Services” on page 42 for more information.
6. Plan for your performance monitoring systems.
7. Plan and define your problem diagnosis procedures.
   See “Problem diagnostic plan strategy” on page 281 for more information.
8. Consider automatic restart management before you install WebSphere Application Server for z/OS.
   See “Automatic restart management” on page 278 for more information.
9. Plan your product dataset and HFS naming conventions.
   See Chapter 5, “Planning for installation,” on page 29 for more information.
10. Install the WebSphere Application Server for z/OS product.
    See Chapter 6, “Installing the product and additional software,” on page 35 for more information.
11. Prepare your z/OS target systems to run WebSphere Application Server for z/OS.
    See Chapter 7, “Preparing the base operating system,” on page 39 for more information.
12. Learn about configuring application serving environments.

See Chapter 8, “Planning for product configuration,” on page 49 for more information.

13. Set up a simple standalone application server to verify system readiness and gain experience with a basic application serving environment.

    See “Building a practice WebSphere Application Server for z/OS cell” on page 84 for more information.
14. Plan and define your system backup procedures.
15. Plan and define your software service procedures.
16. (Optional) Plan for testing and production systems.
17. Plan and configure the application serving environments that you want.

    See Chapter 8, “Planning for product configuration,” on page 49 and Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 285.
18. Enable global security (strongly recommended).
19. Develop and deploy applications.
20. Review WebSphere Application Server for z/OS requirements for application development and client environments.
21. (Optional) Implement Sysplex Distributor, and set up a high-availability environment.
22. (Optional) Expand your application serving environments as needed.
23. Tune system performance.

    See “Skill requirements” on page 13 for more information.

Results

Once you have identified the elements you want to incorporate in your implementation plan, you are ready to install and configure the product.

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.

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.

Product version information

The WebSphere Application Server product contains structural differences from previous versions.

The properties/version directory in the *app_server_root* contains important data about the product and its installed components, such as the build version and build date. This information is included in WAS.product and [component].component files.

Run the historyInfo command to create a report about installed maintenance packages. The historyInfo command creates a report on the console and also creates tracking files in the *app_server_root*/properties/version/history directory.

Time-stamped, detailed logs record each update process in the properties/version/log directory of the *app_server_root*.

This topic describes the XML data files that store product information for WebSphere Application Server products. By default, the document type declarations (DTDs) for these files are in the properties/version/dtd folder of the *app_server_root*, or the server root directory. See the “Product version information” section for more information.

This topic includes the following sections:

Product information files

XML files in the properties/version directory that store version information:

platform.websphere
One file whose existence indicates that a WebSphere Application Server product is installed. An example of the file follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE websphere PUBLIC "websphereId" "websphere.dtd">
<websphere name="IBM WebSphere Application Server" version="7.0"/>
```

The following XML files in the properties/version directory represent installed items and installation events such as product edition, version, component, and build information.

WAS.product

One file whose existence indicates the particular WebSphere Application Server product that is installed. The type of product installed is indicated by the <id> tag. Data in the file indicates the version, build date, and build level.

For example, <id>ND</id>.product indicates that the installed product is WebSphere Application Server Network Deployment. An example of the file follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE product PUBLIC "productId" "product.dtd">
<product name="IBM WebSphere Application Server - ND">
  <id>ND</id>
  <version>7.0.0</version>
  <build-info date="09/03/08" level="s0845.18"/>
</product>
```

component-name.**component**

Any number of component files that each indicate the presence of an installed component, which is part of the product. Data in the file indicates the component build date, build version, component name, and product version. For example, the file might be the activity.component file, which indicates that the activity component is installed. The activity component is part of the Network Deployment product. An example of the file follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE component PUBLIC "componentId" "component.dtd">
<component build-date="08/31/08" build-version="a0838.07"
   name="activity" spec-version="7.0.0.0"/>
```

extension.id.**extension**

Any number of extension files that each indicate the presence of an extension that you install as a user extension, as part of a service engagement, or as installed by a third party product. The *<extension.id>*.extension files are not created, logged, or removed by WebSphere Application Server products.

ptf-id.**ptf**

Any number of maintenance package files that each indicate the presence of an installed refresh pack, fix pack, or interim fix.

XML files in the properties/version/history directory that store version history information files: The following XML files in the properties/version/history directory describe refresh packs, fix packs, and interim fixes that are currently installed. These XML files are related to installation items by the primary ID information, which is shown in the following examples as italicized text.

xxxmaintenance_package_identifierxxx.**ptfDriver**

A driver file has useful information about the entire contents of an interim fix or fix pack.

xxxmaintenance_package_identifierxxx.**ptfApplied**

The applied file has relevant information about the interim fixes or fix packs that are currently applied.

event.history

One file that lists update events that have occurred. An update event is an operation that installs or uninstalls an interim fix or a fix pack. The file is sorted by the date and time of the events that are listed.

Reports

WebSphere Application Server provides the ability to generate ***Version*** reports and History reports from the data in the files. The following report-generation scripts are available in the *app_server_root* bin directory.

Product version reports

The following report generation scripts extract data from XML data files in the properties/version folder:

- versionInfo command

  Lets you use parameters to create a version report on platforms such as AIX® or Linux®, or on Windows® platforms.

- genVersionReport command

  Generates the versionReport.html report file in the bin directory on platforms such as AIX or Linux, or on Windows platforms. The report includes the list of components and installed and uninstalled maintenance packages.

Product history reports

The following report generation scripts extract data from XML data files in the properties/version/history folder:

- historyInfo command

  Lets you use parameters to create a history report on platforms such as AIX or Linux, or on Windows platforms.

- genHistoryReport command

  Generates the historyReport.html report file in the bin directory on platforms such as AIX or Linux, or on Windows platforms. The report includes the list of components and a history of installed and uninstalled maintenance packages.

Logs and component backups

WebSphere Application Server products use two other directories when performing update operations, for logging and backups:

app_server_root **/logs/update**
: The logs directory for product updates.

  The location of log files that describe events that occur during the use of the update installer program.

*app_server_root***properties/version/backup**
: Product updates backup directory

  WebSphere Application Server products back up components before applying interim fixes and fix packs. If you uninstall an interim fix or fix pack, WebSphere Application Server products restore the backed-up component JAR file.

File naming convention

Time stamp
: YYYYMMDD_HHMMSS

  For example: 20050324_211832 is 24-Mar-2004, 9:18:32 pm, GMT. All time stamps are in GMT.

ID Interim fix ID or fix pack ID

  For example: apar6789c is an interim fix ID; PTF_1 is a fix pack ID.

Operation
: install | uninstall

Interim fix log file names
: *timeStamp_fixID_operation*.log

  For example, the Update installer program creates these logs: *app_server_root*logs/update/20050324_211832_apar6789c_install.log and *app_server_root*/logs/update/20050324_211912_apar6789c_uninstall.log

Interim fix component log file names
timeStamp_fixId_componentName_operation.log

For example, the update installer program creates these logs: *app_server_root*/logs/update/20050324_211832_apar6789c_ras_install.log and *app_server_root*/logs/update/20050324_211912_apar6789c_ras_uninstall.log

Fix pack log file names
timeStamp_ptfId_operation.log

For example, the update installer program creates these logs: *app_server_root*/logs/update/20050924_211832_was60_fp1_install.log and *app_server_root*/logs/update/20050924_211912_was60_fp1_uninstall.log

Fix pack component log file names
timeStamp_ptfId_componentName_operation.log

For example, prior to Fix Pack 2: properties/version/log/20050324_211832_was50_fp1_ras_install.log and properties/version/log/20030325_211912_was50_fp1_ras_uninstall.logThe update installer program creates these logs: *app_server_root*/logs/update/20050324_211832_was60_fp1_ras_install.log and *app_server_root*/logs/update/20030325_211912_was60_fp1_ras_uninstall.log

Backup JAR file names
*timeStamp_ptfId_componentName*_undo.jar or *timeStamp_fixId_componentName*_undo.jar

For example: 20020924_211832_apar6789c_ras_undo.jarDo not delete a backup JAR file. You cannot remove a component update if the corresponding backup JAR file is not present.

Update processing might also use a temporary directory if necessary. A Java property specifies this directory as described in the next section.

Directory locations

Product information files are located relative to the WebSphere Application Server product *app_server_root*, or the server root directory.

Default file paths are:

Version directory
app_server_root/properties/version

History directory
app_server_root/properties/version/history

Updates log directory
The update installer program stores log files in the *app_server_root*/logs/update directory.

Updates backup directory
app_server_root/properties/version/backup

DTD directory
app_server_root/properties/version/dtd

Temporary directory
Specified by the java.io.tmpdir Java system property

Operational description

WebSphere Application Server products update the product version history information while performing events that install or uninstall fixes or fix packs. Events that might occur include:

- A WebSphere Application Server product removes an interim fix file from the version directory when it uninstalls the corresponding fix.

- A WebSphere Application Server product adds a file with an extension of .ptf to the version directory to indicate than a refresh pack, a fix pack, or an interim fix is currently installed.
- A WebSphere Application Server product removes a file with an extension of .ptf from the version directory when it uninstalls the corresponding refresh pack, a fix pack, or an interim fix.
- A WebSphere Application Server product adds a driver file with an extension of .ptfDriver to the version/history directory when you run the historyInfo command. A fix pack driver file contains defining information for a fix pack.
- A WebSphere Application Server product adds a fix pack applied file with an extension of .ptfApplied to the version/history directory when you run the historyInfo command. A fix pack application file contains information that identifies component updates that have been applied for a fix pack. The application file also provides links to component log and backup files.
- A WebSphere Application Server product makes entries in the history file, event.history, when it installs or uninstalls a maintenance package.
- A WebSphere Application Server product writes a line about a parent event for each refresh pack, a fix pack, or interim fix that it installs or uninstalls.
- A WebSphere Application Server product stores child component events for each component update that it installs or uninstalls, beneath the corresponding interim fix, fix pack, or refresh pack parent event.
- A WebSphere Application Server product stores one log file in the logs/update directory as it installs or uninstalls one interim fix, fix pack, or refresh pack.
- A WebSphere Application Server product stores one log file in the logs/update directory as it installs or uninstalls an interim fix, fix pack, or refresh pack in response to each component update that occurs.
- A WebSphere Application Server product stores a component backup file in the backup directory for each component update that it installs.
- A WebSphere Application Server product removes a component backup file from the backup directory for each component update that it uninstalls.

Data dictionary

Type Family: WebSphere product family

File Types:
websphere

File Type:
websphere

Elements:

```
name                string     required
version             string     required
```

Persistence:
versionDir/platform.websphere

Type Detail:

The websphere file denotes the presence of WebSphere family products.

Element Detail:

```
websphere.name          The WebSphere product family name.
websphere.version       The WebSphere product family version.
```

```
Type Family:      product

File Types:       product
                  component
                  extension
```

```
File Type:        product

Persistence:      versionDir/WAS.product

Elements:         id                    string     required
                  name                  string     required
                  version               string     required
                  build-info            complex    required

Type Detail:

A product file is placed to denote the presence of a specific
WebSphere family product.
The product ID is embedded in the product file name.

Element Detail:

product.id               The id of the product.
product.name             The name of the product.
product.version          The version of the product.
product.build-info       An element containing build information for
                         the product.

Element Type:     build-info

Elements:         date                  date       required
                  level                 string     required

Type Detail:

A build-info instance details the build of a specific installed
WebSphere family product.

Element Detail:

build-info.date          The date on which the product was build.
build-info.level         The level code of the product's build.

File Type:        component

Persistence:      versionDir/name.component

Elements:         name                  string     required
                  spec-version          string     required
                  build-version         string     required
                  build-date            date       required

File Detail:

A component file denotes the presence of a specific component.
The component name is embedded in the component file name.

Element Detail:

component.name           The name of the component.
component.spec-version   The specification version of the component.
component.build-version  The build level of the component.
component.build-date     The build date of the component.


Type Family:      update

File Types:       ptf
                  ptf-applied

File Type:        ptf
```

```
Persistence:      versionDir/id.ptf

Elements:         id                    string     required
                  short-description     string     required
                  build-version         string     required
                  build-date            date       required
                  component-name        complex    min=1, max=unbounded

Type Detail:

A ptf file denotes the presence of some portion of a specific refresh pack,
fix pack, or interim fix.

The id of the refresh pack, fix pack, or interim fix is embedded in the fix
pack file name.

A ptf file contains a listing of component updates.

When installing a refresh pack, fix pack, or interim fix, you can omit certain
potential component updates, but only when the corresponding component is not
installed.

Examine a separate application file to determine the components that
a particular refresh pack, fix pack, or interim fix updates.

A refresh pack or fix pack can include updates for a number of interim fixes.


Element Detail:

ptf.id                   The ID of the fix pack.

ptf.short-description    A short description of the fix pack.

ptf.build-version        The build version of the fix pack.
                         This is distinct from the build version of
                         component updates contained within the fix pack.

ptf-build-date           The build date of the fix pack.  This is distinct
                         from the build version of the component updates
                         contained within the
                         fix pack.

ptf.component-name       A list of components.



File Type:        ptf-applied

Persistence:      versionDir/id.ptfApplied

Elements:         ptf-id                string     required
                  component-applied     complex    min=0, max=unbounded

Type Detail:

A ptf-applied collection specified what components have been updated for
the refresh pack, fix pack, or interim fix as specified by the ID.

Element Detail:

ptf-applied.ptf-id         The ID of the refresh pack, fix pack, or interim fix
                           for which applieds are recorded.

ptf-applied.component-applied  The list of recorded applications.
```

```
Element Type:     component-applied

Elements:         component-name        string     required
                  update-type           enum       required [enumUpdateType]
                  log-name              anyURL     required
                  backup-name           anyURL     required
                  time-stamp            date       required

Type Detail:

An applied instance is present to indicate the application of an
update for a particular interim fix, fix pack, or refresh pack to a
particular component.

(The particular interim fix, fix pack, or refresh pack is specified by
the applied parent.)  An applied provides sufficient information
to undo itself.

The elements of an applied are copies of values from update
events.

Element Detail:

component-applied.component-name   The name of the component which was updated.

component-applied.update-type      The type of the component update.

component-applied.log-name         The name of the log file that was generated by
                                   this application.

component-applied.backup-name      The name of the backup file that was generated by
                                   this application.

component-applied.time-stamp       The time of this application (the ending time of
                                   the corresponding update event).



Enum Type:        enumUpdateType

Values:           0 add
                  1 replace
                  2 remove
                  3 patch

Type Detail:

An update type instance specifies the type of an update.  An 'add' update adds
a component into an installation.  A 'replace' update replaces a particular
version of a component with a different version of that component.  A 'remove'
update removes a component.  A 'patch' update performs a limited update to a
component, in particular, without changing the version of the component.

When adding a component, that component may not already be present.
When replacing or removing a component, that component must be present.
When patching a component, that component must be present.

When replacing or removing a component, or when patching a component, usually,
at least one version prerequisite will be specified for the component update.

Value Detail:

enumUpdateType.add       Specifies that an update adds a component.

enumUpdateType.replace   Specifies that an update replaces a component.

enumUpdateType.remove    Specifies that an update removes a component.
```

```
enumUpdateType.patch     Specifies that an update modifies a component, but
                         does not change its version.


Type Family:      history

File Type:        event-history

Persistence:      historyDir/event.history

Elements:         update-event          complex    min=0, max=unbounded

Type Detail:

One event history is provided for a websphere product family installation.
This event history contains history of update events, corresponding with
the actual update events for that product family.

Element Detail:

event-history.update-event  The list of update events for the websphere
                            product family.  The top level events are refresh pack,
                            fix pack, and interim fix events, each containing one
                            or more component events.

Element Type:     update-event

Elements:         event-type            enum       required [enumEventType]
                  parent-id             string     required
                  id                    string     required
                  update-type           enum       required [enumUpdateType]
                  primary-content       anyURI     required
                  update-action         enum       required [enumEventAction]
                  log-name              anyURI     required
                  backup-name           anyURI     required
                  start-time-stamp      dateTime   required
                  result                string     required
                  update-event          complex    optional

Type Detail:

An update event denotes a single update action, applying to either a
fix, a fix pack, a refresh pack, or a component, according to the set
event type.

Element Detail:

update-event.event-type        The type of this event, either a refresh pack, fix
                               pack, or an interim fix type event, or a component
                               type event.

update-event.parent-id         This element is present only for component
                               events. The ID of the parent interim fix, fix
                               pack, or refresh pack of this event.

update-event.id                The ID of the interim fix, fix pack, refresh pack,
                               or component that was updated, interpreted according
                               to the type of the event.

update-event.update-type       The type of update for an update event.

update-event.update-action     The type of action for this event.

update-event.log-name          The name of the log file that was generated
                               for this event.
```

```
update-event.backup-name       The name of the backup file that was generated
                               for this event.

update-event.start-time-stamp  The XML timestamp of the starting time of the
                               event.  This timestamp follows the XML timestamp
                               format, meaning that time zone information is
                               included.

update-event.result            The result of the update.

update-event.update-event      A collection of child events.  This collection is
                               used for interim fix and fix pack type events.
                               This collection is empty for component type events.


Type Detail:

An event type instance specifies the type of an update event, which is either
a refresh pack, fix pack, or interim fix (ptf) event or a component event. The
interpretation of particular event elements depends on the set event type.

Value Detail:

EventType.ptf        Specifies that an event is for a refresh pack, fix pack,
                     or interim fix update.

EventType.component  Specifies that an event is for a component update.

Enum Type:        update-action

Values:           0 Install
                  1 Uninstall

Type Detail:

An event action instance specified the operation performed by an update, which
can be an install or uninstall operation.


Value Detail:

enumEventAction.install              Specifies that an event is an install
                                     operation.

enumEventAction.uninstall            Specifies that an event is an uninstall
                                     operation.

Enum Type:        enumUpdateType

Values:           0 Add
                  1 Replace
                  2 Remove
                  3 Patch

Type Detail:

An update type instance specifies the type of a component update.

An 'add' update adds a component into an installation.

A 'replace' update replaces a particular version of a component with
a different version of that component.

A 'remove' update removes a component.

A 'patch' update performs a limited update to a component,
in particular, without changing the version of the component.
```

```
To add a new component, the component must not exist.
To replace or remove a component, the component must exist.
To patch a component, the component must exist.

When replacing or removing a component, or when patching a component,
usually, at least one version prerequisite is specified for the
component update.

Value Detail:

enumUpdateType.add       Specifies that an update adds a component.

enumUpdateType.replace   Specifies that an update replaces a component.

enumUpdateType.remove    Specifies that an update removes a component.

enumUpdateType.patch     Specifies that an update modifies a component, but
                         does not change its version.

Enum Type:        enumEventResult

Values:           0 Succeeded
                  1 Failed
                  2 Cancelled

Type Detail:

An event result instance denotes a particular result for an update event.
The result indicates success, failure, or cancellation.

Value Detail:

enumEventResult.succeeded  Specifies that the operation was successful.

enumEventResult.failed     Specifies that the operation failed.

enumEventResult.cancelled  Specifies that the operation was cancelled.
```

Installation: Resources for learning

Use the following links to find relevant supplemental information about installation and customization. The information resides on IBM and non-IBM Internet sites, whose sponsors control the technical accuracy of the information.

These links are provided for convenience. Often, the information is not specific to the IBM WebSphere Application Server product, but is useful in all or in part for understanding the product. When possible, links are provided to technical papers and Redbooks that supplement the broad coverage of the release documentation with in-depth examinations of particular product areas.

One important link is:

How to buy WebSphere Application Server software

This IBM Web site describes pricing and technical details. If you have already purchased the software, view links to additional information about:

- Planning, business scenarios, and IT architecture
- Programming instructions and examples
- Programming specifications
- Administration
- Support

Planning, business scenarios, and IT architecture

- Supported hardware and software

  The official site for determining product prerequisites for hardware and software for all WebSphere Application Server products.
- IBM developerWorks WebSphere

  The home of technical information for developers working with WebSphere products. You can download WebSphere software, take a fast path to developerWorks zones, such as VisualAge® Java or WebSphere Application Server, learn about WebSphere products through a newcomers page, tutorials, technology previews, training, and Redbooks, get answers to questions about WebSphere products, and join the WebSphere community, where you can keep up with the latest developments and technical papers.
- IBM WebSphere Application Server library and information centers Web site

  The IBM WebSphere Application Server Library Web site contains links to all WebSphere Application Server information centers, for all versions. It also lets you access each information center in your native language.
- IBM WebSphere Application Server home page

  The IBM WebSphere Application Server home page contains useful information, including support links and downloads for maintenance packages, APARs, tools, and trials.
- IBM WebSphere software platform home page

  The IBM WebSphere software platform home page introduces WebSphere products and describes how companies can easily transform to an e-business, with software that can grow as fast as the business it supports.
- WebSphere Application Server Edge components library and information centers Web site

  The information center for WebSphere Application Server Edge components contains complete documentation for the Caching Proxy and the Load Balancer.

Programming instructions and examples

- IBM developerWorks

  IBM developerWorks contains many excellent resources for developers, including tutorials on Web development-related topics. There is an excellent tutorial on the JDBC API.
- IBM Redbooks

  The IBM Redbooks site contains many documents that are related to WebSphere Application Server.

Programming specifications

- Java EE information

  For more information about Java Platform, Enterprise Edition specifications, visit the Sun site.

Administration

- WebSphere technical library on developerWorks

  The WebSphere library includes a wide range of content, including technical articles, downloads, product documentation, and tutorials
- The IBM Terminology Web site

  The IBM Terminology Web site consolidates the terminology from many IBM products in one convenient location. In addition to base computer terminology, terms and definitions from IBM brands and product families are included and explained.

Support

- Steps to getting support for WebSphere Application Server

  Whether you are a new user looking for basic information, or an experienced user looking for a specific workaround, you can benefit immediately from IBM's extensive Web-based support. Download fixes, search on keywords, find how-to information, and possibly solve a problem -- all before contacting IBM Software Support directly.
- WebSphere Application Server for z/OS Support page

Take advantage of the Web-based Support and Service resources from WebSphere Application Server to quickly find answers to your technical questions. Easily access the latest downloads, find workarounds to technical problems, or register to receive e-mail from IBM Support.

- IBM e-server Support: Fix Central

  A Web facility for downloading fixes for hardware and operating systems, including z/OS and IBM i.
- Adobe® Acrobat Web site

  This Adobe Web site offers a free download of the Adobe Acrobat Reader product.

Chapter 5. Planning for installation

Use this task to prepare to install WebSphere Application Server for z/OS product code.

Before you begin

Print and review “Creating your implementation plan” on page 14. Assemble a team of people to install and configure the product. Be sure that the team has the skills needed to plan, install, and configure WebSphere Application Server for z/OS. See “Skill requirements” on page 13 for more information.

About this task

You must completely install the product code for WebSphere Application Server for z/OS before you can set up an application serving environment. Obtain product code from IBM in one of the following formats:

- An **IBM ServerPac or SystemPac**, which consists of loadable product libraries and corresponding SMP/E datasets. A ServerPac or SystemPac contains program libraries with integrated maintenance for one or more products, which include a base operating system, such as z/OS, if desired. Program library datasets are loaded to disk as part of the ServerPac or SystemPac installation. After installation, perform maintenance with SMP/E.
- An **IBM Custom-Build Product Delivery Option (CBPDO)**, which consists of SMP/E relfiles. A CBPDO contains SMP/E relfiles and maintenance for one or more products. Install each product using SMP/E commands (APPLY / ACCEPT) or the corresponding panels. After installation, perform maintenance with SMP/E.

Perform the tasks in this section before you install the WebSphere Application Server for z/OS product code. By planning your product code placement and naming, you can ease future product maintenance and migration tasks.

1. Make sure that the z/OS system on which you will install WebSphere Application Server for z/OS meets the hardware and software requirements. See “Driving system requirements” on page 10 for more information.
2. Identify the software delivery option you will use. To review your product delivery options see “IBM SystemPac or ServerPac” on page 35 or “IBM Custom-Build Product Delivery Offering” on page 36 for more information.
3. Learn about WebSphere Application Server product datasets, and plan a naming convention. See “Product datasets” on page 30 for more information.
4. Learn about WebSphere Application Server product directories, and plan a mount point convention. See “Product file system” on page 32 for more information.
5. Decide whether to install the WebSphere Application Server Version 7.0 Optional Materials feature.

   This feature must be installed in order to install and use feature packs and other interim deliverables.
6. Decide whether to install the DMZ Secure Proxy Server for WebSphere Application Server Version 7.0.

   The DMZ Secure Proxy Server must be installed in order to run a secure proxy server on a z/OS system that might not include the WebSphere Application Server for z/OS product. The DMZ Secure Proxy Server has its own product datasets, and it can be installed in an SMP/E environment that is separate from that of the WebSphere Application Server for z/OS base product and Optional Materials feature.

What to do next

When you have finished the planning process, you are ready to begin installing the product. See Chapter 6, “Installing the product and additional software,” on page 35.

Product datasets

This article describes the WebSphere Application Server for z/OS product datasets and recommends a product dataset naming convention.

WebSphere Application Server for z/OS product code resides in MVS™ partitioned datasets, which contain the product datasets, and the MVS hierarchical file system directories, which contain the product directory and its subdirectories. The default high-level qualifier for the product datasets is BBO.

In this and other articles in the information center, *was_hlq* is used to represent the high-level data set name qualifier for a particular set of WebSphere Application Server for z/OS product datasets.

Note: Beginning with WebSphere Application Server for z/OS Version 7.0, the SBBOLOAD and SBBOLD2 datasets no longer exist by default. This is because the load modules are now in the file system. If you want to switch a configuration from using load modules in the file system to using load modules in a dataset, you can use the tool described in “switchModules command” on page 383.

Product dataset contents

The WebSphere Application Server for z/OS product datasets are divided into target datasets (used during product customization and execution) and distribution libraries (used to ″back off″ maintenance if necessary).

- **WebSphere Application Server for z/OS target libraries**

was_hlq.SBBOEXEC	CLIST scripts
was_hlq.SBBOJCL	JCL for installation jobs
was_hlq.SBBOMSG	Message translation skeletons

- **WebSphere Application Server for z/OS distribution libraries**

was_hlq.ABBOANT	HFS files
was_hlq.ABBOEBCD	HFS files (EBCDIC)
was_hlq.ABBOINC	Include files
was_hlq.ABBOJAR	JAR files
was_hlq.ABBOJCL	JCL for installation jobs
was_hlq.ABBOMAC	Assembler macros
was_hlq.ABBOMSG	Message translation skeletons
was_hlq.ABBOEXEC	CLIST scripts
was_hlq.ABBOLOAD	Load modules
was_hlq.ABBOMIG	IPCS formatters
was_hlq.ABBOZAR	Administrative console

- **WebSphere Application Server for z/OS Optional Materials target libraries**

was_hlq.SIWOEXEC	CLIST scripts
was_hlq.SIWOJCL	JCL for installation jobs

- **WebSphere Application Server for z/OS Optional Materials distribution libraries**

was_hlq.AIWOEXEC	CLIST scripts
was_hlq.AIWOJCL	JCL for installation jobs

- **DMZ Secure Proxy Server for WebSphere Application Server target libraries**

was_hlq.SDYZEXEC	CLIST scripts
was_hlq.SDYZJCL	JCL for installation jobs
was_hlq.SDYZMSH	Message translation skeletons

- **DMZ Secure Proxy Server for WebSphere Application Server distribution libraries**

was_hlq.ADYZANT	HFS files
was_hlq.ADYZEBCD	HFS files (EBCDIC)
was_hlq.ADYZEXEC	CLIST scripts
was_hlq.ADYZINC	Include files
was_hlq.ADYZJAR	JAR files
was_hlq.ADYZJCL	JCL for installation jobs
was_hlq.ADYZMSG	Message translation skeletons
was_hlq.ADYZLOAD	Load modules
was_hlq.ADYZMIG	IPCS formatters

See WebSphere Application Server for z/OS: Program Directory (GI11-2825) for allocation information about each target library and distribution library. Updates to this information are included in the Preventive Service Planning (PSP) bucket for each release of WebSphere Application Server for z/OS.

Product dataset naming restrictions

The IBM ServerPac and SystemPac and the IBM Custom-Build Product Delivery Option allow you to rename product datasets during installation. In addition, the IBM ServerPac and SystemPac allow you to merge members from similar target libraries into a single dataset.

Product dataset naming convention

As noted above, certain WebSphere Application Server for z/OS data sets must have the same high-level dataset name qualifier in order for the product to function correctly. Product maintenance and migration is easier if all product datasets have the same high-level qualifier.

On the other hand, in order to continue to run WebSphere Application Server for z/OS while applying maintenance, you must have at least two copies of the product data sets: one for the running application execution environment and one to which service is applied.

We recommend you choose a middle level qualifier for each separate release and maintenance level of WebSphere Application Server for z/OS. This middle level qualifier can reflect a very simple test/production distinction, such as with ″BBO.V7PROD.*″ or ″BBO.V7TEST.*″, or can include specific service level information, such as with ″WAS.W700102.*″ or ″WAS.W700103.*″.

There are many places where you must specify the product dataset names, so, to avoid undue confusion, use the simplest dataset naming scheme that accomplishes your maintenance goals.

Related reference

“switchModules command” on page 383
You can use the switchModules command to switch a configuration between using load modules in the file system and using load modules in a dataset.

Product file system

The product directory and all of its subdirectories reside in the same hierarchical file system (HFS). The default product directory is represented by the version or release. Throughout the product and documentation, *install_root* is used to represent the fully qualified path name.

WebSphere Application Server for z/OS product code resides in MVS-partitioned product datasets and MVS file system (the product directory and its subdirectories).

Product directory

All WebSphere Application Server for z/OS product files reside in the product directory and its subdirectories. The default product directory is /usr/lpp/zWebSphere/V7R0. Throughout the product and documentation, *install_root* is used to represent the fully qualified path name of the WebSphere Application Server for z/OS product directory.

Locate the product directory and all of its subdirectories in the same hierarchical file system (HFS) or zSeries® file system (ZFS) dataset. This dataset can be the same as the z/OS root or version dataset, which is not recommended, or a separate dataset that is used just for WebSphere Application Server for z/OS. The installation jobs and program directory assume that such a separate data set is allocated. This dataset is referred to as *was_hlq*.SBBOHFS, where *was_hlq* represents the product dataset name high-level qualifiers. This directory gets created during the installation process.

Refer to the Program Directory on the WebSphere Application Server library Web page for more details.

Optional Materials product directory

The WebSphere Application Server for z/OS Optional Materials files reside in the Optional Materials product directory and its subdirectories. The default Optional Materials product directory is /usr/lpp/zWebSphere_OM/V7R0. Each interim deliverable (such as a feature pack) has its own subdirectory in the Optional Materials product directory.

Refer to the Program Directory on the WebSphere Application Server library Web page for more details.

DMZ Secure Proxy Server product directory

The DMZ Secure Proxy Server for WebSphere Application Server files reside in the DMZ Secure Proxy Server product directory and its subdirectories. The default DMZ Secure Proxy Server product directory is /usr/lpp/zWebSphere_SPS/V7R0.

Refer to the Program Directory on the WebSphere Application Server library Web page for more details.

Product directory and configuration directory

Each WebSphere Application Server for z/OS application serving environment (standalone application server node or Network Deployment cell) has configuration files in one or more WebSphere configuration directories. These configuration directories are created through the configuration process and contain symbolic links to files in the product directory.

WebSphere Application Server for z/OS application serving environments that are enabled for interim deliverables such as feature packs have symbolic links to files in the Optional Materials product directory.

DMZ secure proxy servers and secure proxy administrative agents have symbolic links to files in the DMZ Secure Proxy Server product directory.

Using indirection to isolate product directories

Instead of pointing directly to these product directories, application serving environments can point to an intermediate symbolic link, which in turn points to a particular product directory. This level of indirection allows you to switch to a new server level of WebSphere Application Server for z/OS or the DMZ Secure Proxy server by stopping the servers that use that intermediate symbolic link, changing the link to point to the new product directory, and restarting the affected servers.

The customization process allows for automatic creation of these intermediate symbolic links.

Chapter 6. Installing the product and additional software

Use this task to install WebSphere Application Server for z/OS product code.

Before you begin

Complete the steps in Chapter 5, “Planning for installation,” on page 29.

About this task

The product code for WebSphere Application Server for z/OS is installed using either an IBM ServerPac/SystemPac or an IBM Custom-Built Product Delivery Option (CBPDO). This section of the documentation provides guidance on using these two vehicles to install the WebSphere Application Server for z/OS product.

Perform the tasks in this section to install the WebSphere Application Server for z/OS product code.

1. Order an IBM ServerPac/SystemPac or IBM CBPDO that contains the appropriate WebSphere Application Server for z/OS product.
2. Follow the instructions for the delivery vehicle that you choose:
   - “IBM SystemPac or ServerPac”
   - “IBM Custom-Build Product Delivery Offering” on page 36
3. If you plan to use any of the WebSphere Application Server interim deliverables, verify that the optional materials were installed (if you use SystemPac or ServerPac) or install them according to the instructions in the Program Directory.
4. If you plan to use the DMZ Secure Proxy Server for WebSphere Application Server, verify that the DMZ Secure Proxy Server product files were installed (if you use SystemPac or ServerPac) or install them according to the instructions in the Program Directory.
5. Save the installation materials for later use during product maintenance.

What to do next

When you have finished the installation process, you are ready to prepare your target systems for WebSphere Application Server for z/OS. Read Chapter 7, “Preparing the base operating system,” on page 39 for more information.

IBM SystemPac or ServerPac

An IBM CustomPac (SystemPac, ServerPac or ProductPac®) is a set of preloaded product datasets bundled with an IBM dialog that is used to load the data sets to disk and perform initial customization. In general, SMP/E work is not required during installation of a CustomPac offering. Instead, SMP/E data sets that correspond to the CustomPac service level are loaded onto the disk along with the product datasets. You can still use SMP/E to install preventive and corrective service after CustomPac installation.

If you use an IBM SystemPac or ServerPac, follow the instructions in the copy of *ServerPac: Installing your Order* that ships with your SystemPac or ServerPac.

See *ServerPac: Using the Installation Dialog* (SA22-7815) for information about the ISPF dialog used to install a SystemPac or ServerPac.

Note:

- Be sure to choose a product dataset naming convention that allows you to keep and maintain at least two copies of product libraries for maintenance purposes.

- If you are installing from a driving system, make sure that the maintenance level of the target system meets requirements for WebSphere Application Server for z/OS.
- When installation is complete, make sure that the product datasets are available to your z/OS target systems and the product code HFS is mounted at /usr/lpp/zWebSphere/V7R0 or at a similar mount point of your choice on each target system.
- If the optional materials are installed, make sure that the optional materials product code file system is mounted at /usr/lpp/zWebSphere_OM/V7R0 or at a similar mount point of your choice on each target system.
- If the DMZ Secure Proxy Server is installed, make sure that the DMZ Secure Proxy Server product file system is mounted at /usr/lpp/zWebSphere_SPS/V7R0 or at a similar mount point of your choice on each target system where a DMZ secure proxy server is to run.

  The DMZ secure proxy server does not use the ″normal″ WebSphere Application Server product file system or the optional materials.

For further information, see the following:

- eSupport Web site at http://www.ibm.com/software/webservers/appserv/zos_os390/support/
- PSP buckets
- IBM Software Support Center

IBM Custom-Build Product Delivery Offering

An IBM Custom-Build Product Delivery Offering (CBPDO) is a set of product tapes for one or more IBM software products that is bundled with cumulative service. Install the products and service on your system using SMP/E.

If you use CBPDO, follow the instructions in the copy of *WebSphere Application Server for z/OS: Program Directory* that ships with your order.

Note:

- Be sure to choose a product dataset naming convention that allows you to keep and maintain at least two copies of product libraries for maintenance purposes.
- If you are installing from a driving system, make sure that the maintenance level of the target system meets requirements for WebSphere Application Server for z/OS.
- When installation is complete, make sure that the product datasets are available to your z/OS target systems and the product code HFS is mounted at /usr/lpp/zWebSphere/V7R0 or a similar mount point of your choice on each target system.
- If the optional materials are installed, make sure that the optional materials product code file system is mounted at /usr/lpp/zWebSphere_OM/V7R0 or at a similar mount point of your choice on each target system.
- If the DMZ Secure Proxy Server is installed, make sure that the DMZ Secure Proxy Server product file system is mounted at /usr/lpp/zWebSphere_SPS/V7R0 or at a similar mount point of your choice on each target system where a DMZ secure proxy server is to run.

  The DMZ secure proxy server does not use the ″normal″ WebSphere Application Server product file system or the optional materials.

For further information, see the following:

- eSupport Web site at http://www.ibm.com/software/webservers/appserv/zos_os390/support/
- PSP buckets
- IBM Software Support Center

Installing and updating Websphere Customization Tools

You can install the most current release of WebSphere Customization Tools Version 7.0 on a workstation running the Windows or Linux Intel® operating system so that you can use the Profile Management Tool and the z/OS Migration Management Tool to generate the jobs and instructions for creating and migrating profiles.

- If the latest release of WebSphere Customization Tools Version 7.0 is on your product disk, install it.
- If the latest release of WebSphere Customization Tools Version 7.0 is not on your product disk, perform the following tasks:
  1. Go to Recommended fixes for WebSphere Application Server.
  2. Look under **Version 7.0** for a link to the WebSphere Customization Tools Version 7.0 download page.
  3. Go to that Web page, and download the latest WebSphere Customization Tools Version 7.0 package.
  4. **Optional:** Uninstall any earlier releases of WebSphere Customization Tools Version 7.0 from your system.

     Note: You can have multiple copies of WebSphere Customization Tools concurrently installed. If you want to do this (to make sure that the new version is working before deleting the old version for example), the only requirement is that you install each version at a different location.
  5. Install the new WebSphere Customization Tools Version 7.0 package.

Uninstalling Websphere Customization Tools

You can uninstall WebSphere Customization Tools Version 7.0 from a workstation running the Windows or Linux Intel operating system.

About this task

Note: You can have multiple copies of WebSphere Customization Tools concurrently installed. If you want to do this, the only requirement is that you install each version at a different location.

- Windows Use **Add or Remove Programs** from the control panel.
- Windows Linux Run the uninstall command.
  - Windows Run the following command:

    WCT_install_root\uninstall_wct\uninstall.exe
  - Linux Perform the following actions:
    1. Go to the *WCT_install_root*/uninstall_wct directory.
    2. Run the following command:

       ./uninstall
    3. Enter the root password if necessary.

What to do next

You must manually delete the residual files in the *WCT_install_root* directory before attempting to reinstall another instance of Websphere Customization Tools to the same location.

Chapter 7. Preparing the base operating system

Use this task to prepare your z/OS target systems for WebSphere Application Server for z/OS.

Before you begin

Complete the steps in Chapter 6, “Installing the product and additional software,” on page 35.

Identify the z/OS systems on which you plan to run WebSphere Application Server for z/OS.

About this task

The WebSphere Application Server for z/OS product makes extensive use of the underlying z/OS operating system services for security, reliability, and performance.

After you install the WebSphere Application Server for z/OS product code, perform the tasks in this section to prepare your z/OS target systems to run WebSphere Application Server for z/OS.

Note: Target systems are the systems on which WebSphere Application Server for z/OS will actually run. The driving system, on which the WebSphere Application Server for z/OS product code installation is performed, might or might not also be a target system.

1. Identify the first z/OS target system on which you plan to create a WebSphere Application Server for z/OS application serving environment.
2. Print off a copy of “Checklist: Preparing the base operating system” on page 46. Use this worksheet to identify which of the following steps have been completed for the target system and record information you will need during product configuration.
3. Prepare z/OS operating system settings. See “Preparing z/OS to run WebSphere Application Server” for detailed instructions.
4. Prepare z/OS sysplex settings. See “Preparing the sysplex” on page 41 for detailed instructions.
5. Prepare the z/OS job entry subsystem (JES2 or JES3). See “Preparing JES2 or JES3” on page 42 for detailed instructions.
6. Identify TCP/IP resources you want to use and prepare your network. See “Preparing TCP/IP” on page 44 for more information.
7. Set up Resource Recovery Services (RRS). See “Preparing Resource Recovery Services” on page 42 for more information.
8. Set up your SAF-compliant security package. See “Preparing the security server (RACF)” on page 44 if you will use the z/OS Security Server. If you will use another SAF-compliant security product, consult the product’s manufacturer for assistance.
9. Repeat these steps for each z/OS target system on which you plan to run WebSphere Application Server for z/OS.
10. Keep the worksheets you filled out as you will need some of the information you recorded on them during product configuration.

What to do next

When you have completed this task for each z/OS target system, you are ready to plan your WebSphere Application Server for z/OS application serving environments on these target systems. See Chapter 8, “Planning for product configuration,” on page 49 for more information.

Preparing z/OS to run WebSphere Application Server

1. Make sure that all software prerequisites listed in “Target system requirements” on page 10 are met.

2. Make sure that the UNIX System Services environment is active and that the BPXPRMxx settings in effect meet or exceed the following minimum values:

   MAXTHREADS: 10000
   MAXTHREADTASKS: 5000
   MAXFILEPROC: 10000
   MAXSOCKETS (AF_INET domain): 12000
   SHRLIBRGNSIZE: 67000000 (134000000 recommended)

3. Make sure that each WebSphere Application Server for z/OS server address space, as well as OMVS or batch job address spaces that run Java virtual machines, have access to enough virtual memory below the 2-gigabyte bar. (A Java virtual machine requires at least 250M of virtual memory, for example.) We recommend that all WebSphere Application Server address spaces be given at least 1024M of virtual memory.

   To do this: Specify REGION=0 (or a suitably large value, such as 1500M) for all batch job, started task and WLM job steps for WebSphere Application Server.

   Either specify MAXASSIZE(2147483647) or some similarly large value in BPXPRMxx to provide a large system-wide default address space size for Unix System Services address spaces, or set the ASSIZEMAX value in RACF (or similar security system) for each WebSphere Application Server for z/OS client or server user ID, including IDs used to run the batch Postinstaller or similar processes:

   ```
   ALTUSER WASUTIL1  OMVS(ASSIZEMAX(1073741824))  to allow WASUTIL1 a 1-gigabyte address space
   ```

4. If you use localization and alternate code pages with UNIX System Services, make sure that all WebSphere Application Server for z/OS server, administrator and client user IDs (any user IDs that run WebSphere Application Server for z/OS scripts) are run with environment variables LANG and LC_ALL both set to the same locale based on code page IBM-1047. Settings based on any other code page can cause the scripts to fail. See ″Changing the Locale in the Shell″ in *UNIX System Services User's Guide* for more information.

5. Make sure that the /tmp directory has at least 20 megabytes of free space.

   WebSphere Application Server for z/OS makes extensive use of the /tmp directory.

   You can use the `df -kP /tmp` shell command to show the number of available 1K blocks in the /tmp directory HFS. Divide the number of available 1K blocks by 1024 to determine the number of megabytes of free space.

   If your /tmp directory resides in a permanent read-write HFS, use the confighfs command in /usr/lpp/dfsms/bin to extend it as necessary. For example, the following command will add an additional 10 MB of space to the HFS in which /tmp resides:

   ```
   /usr/lpp/dfsms/bin/confighfs -x 10m /tmp
   ```

   If your /tmp directory resides in a temporary file system (TFS), modify the MOUNT statement in BPXPRMxx that defines it to add additional space. To define a 20 MB TFS and mount it at /tmp, for example, use the following MOUNT command:

   ```
   MOUNT FILESYSTEM('/TMP') TYPE(TFS) MOUNTPOINT('/tmp') PARM('-s 20')
   ```

   Note: If you do not specify a space ('-s') value, then the undesirably small default of 1 megabyte will be used.

6. Determine the full dataset names of the following system datasets used by WebSphere Application Server for z/OS:

   SCEERUN
   Language Environment® runtime library

   SCEERUN2
   Language Environment runtime library

   SIEALNKE
   System SSL runtime library

SCLBDLL2
64-bit support code

Also, determine whether these datasets are in the system link pack area (LPA) or link list. Record this information on the worksheet.

7. Make sure that all the following datasets are APF authorized:
   - cee_hlq.SCEERUN
   - cee_hlq.SCEERUN2
   - sys_hlq.SIEALNKE
   - clb.SCLBDLL2
8. Make sure that any IEFUSI or JES2/JES3 exits on your system do not restrict WebSphere Application Server for z/OS address spaces to an address space size of less than 512 MB. Each WebSphere Application Server for z/OS address space should have a region size of at least 512 MB. All WebSphere Application Server for z/OS cataloged procedures are shipped with a default of REGION=0M.
9. Make sure that the TSO segment default region size for WebSphere Application Server for z/OS installer and administrator TSO user IDs is at least 128 MB.

Preparing the sysplex

About this task

WebSphere Application Server for z/OS uses a number of z/OS sysplex services. Therefore, each target system used to run WebSphere Application Server for z/OS must be either a monoplex (single system sysplex) or a member of a sysplex. For more information, see *z/OS MVS Setting Up a Sysplex* (SA22-7625).

Connect systems in a sysplex with channel-to-channel (CTC) communications or through a coupling facility, which is a special logical partition used to share data between sysplex members. Couple datasets on DASD are also used for sysplex coordination.

WebSphere Application Server for z/OS uses the System Logger, an MVS component that allows applications to log data in a sysplex, to log error and trace information and provide XA transaction logging. The System logger creates and manages log streams, which are written first to a coupling facility or local in-memory buffer, then transferred to log datasets on DASD for longer term access. Log streams that are written to local buffers rather than to a coupling facility are called DASD-only log streams.

Follow these steps to prepare your system for a sysplex.

1. Determine if your z/OS target system is already configured as a sysplex.
   a. If so, continue on to the next step.
   b. If not, follow the instructions in *z/OS MVS Setting Up a Sysplex* (SA22-7625) to configure it as a monoplex. Record the sysplex name for later use.
2. Determine if System Logger is already in use on your system.
   a. If so, continue on to the next step.
   b. If not, follow the instructions in the section ″Preparing to Use System Logger Applications″ in *z/OS MVS Setting Up a Sysplex* (SA22-7625).
3. Decide whether WebSphere Application Server for z/OS log streams should reside in a coupling facility or local in-memory buffers. Record the SMS data class, SMS storage class and dataset name prefix to be used for log datasets. If WebSphere Application Server for z/OS log streams will reside in a coupling facility, choose the structure name to be used.

Preparing JES2 or JES3

About this task

WebSphere Application Server for z/OS uses job entry subsystem (JES2/JES3) services like any other MVS application.

1. Identify the cataloged procedure library or libraries (proclibs) that you will use to hold cataloged procedures for WebSphere Application Server for z/OS. You might need to use separate proclibs for each system in a sysplex.
2. If your system uses JES2 EXIT06 or JES3 IATUX03 to control specification of the REGION= value on JOB or EXEC statements, make sure that this control is relaxed for WebSphere Application Server for z/OS address spaces.
3. If you plan to send WebSphere Application Server for z/OS trace output to the JES spool, make sure you have adequate spool space available. WebSphere Application Server for z/OS address spaces can produce a large number of trace records when tracing is activated.

Preparing Resource Recovery Services

WebSphere Application Server for z/OS uses Resource Recovery Services (RRS) to support two-phase transaction commit.

About this task

Note: RRS must be up and running before WebSphere Application Server for z/OS servers are started. See *z/OS MVS Programming: Resource Recovery* (SA22-7616) for more information.

Normally, all systems in a sysplex share a common set of RRS logs for syncpoint processing. If you want to associate specific systems in a sysplex for syncpoint processing, you can specify a log group name when you start RRS. The default log group name is the sysplex name. If you specify a different log group name when you start RRS, it will coordinate syncpoint processing with all systems in the sysplex that use the same RRS log group name.

Resource recovery services log streams

RRS uses five log streams that are shared by the systems in the log group. Every MVS image that runs RRS needs access to the coupling facility and the DASD on which are defined the system logger log streams for its log group.

Note: You can define RRS log streams as coupling facility log streams or as DASD-only log streams.

If using coupling facility log streams, the RRS images on different systems in a sysplex run independently but share log streams to keep track of the work. If a system fails, an instance of RRS on a different system in the sysplex can use the shared logs to take over the failed system's work.

Use DASD-only log streams only in either single system sysplexes with one RRS image or a sysplex in which information should not be shared among RRS images.

The following list summarizes the RRS logs. In the list, *lgname* is the log group name. The default log group name is the sysplex name.

ATR.*lgname***.ARCHIVE**
: Information about completed units of recovery (URs). This log stream is recommended but optional.

ATR.*lgname***.RM.DATA**
: Information about the resource managers using RRS services.

ATR.*lgname***.MAIN.UR**
The state of active URs. RRS periodically moves this information into the RRS delayed UR state log when UR completion is delayed.

ATR.*lgname***.DELAYED.UR**
The state of active URs when UR completion is delayed.

ATR.*lgname***.RESTART**
Information about incomplete URs needed during restart. This information enables a functioning RRS instance to take over incomplete work left over from an RRS instance that failed.

In a multiple-system sysplex, RRS log streams should normally reside in a coupling facility.

All RRS transaction logging for WebSphere Application Server for z/OS will occur solely in the DELAYED.UR log stream. You can still configure your MAIN.UR log stream so that it can handle a production workload in case you deploy a new container or the WebSphere Application Server for z/OS infrastructure changes. WebSphere Application Server for z/OS has no significant impact on the RM.DATA or RESTART logs.

Use the following steps to configure RRS.

1. Copy the RRS cataloged procedure, ATRRRS, from SYS1.SAMPLIB to SYS1.PROCLIB (or another proclib in the MSTJCLxx concatenation), and rename it RRS.

   If you want, you can set the log group name (GNAME) in the RRS cataloged procedure to a specific value. If you will share the ATRRRS proc among several systems, however, you might prefer to set the log group name at RRS startup or use a system variable in IEASYMxx to set each system's RRS log group name.
2. Establish the dispatching priority of the RRS address space.

   The best way to control RRS's dispatching priority is through the workload manager (WLM). IBM recommends that you put RRS in the SYSSTC service class. The service class you choose must give RRS a dispatching priority greater than or equal to the dispatching priority of applications and resource managers that use RRS. SYSSTC will usually accomplish this. For information about system-provided service classes, see *z/OS MVS Planning: Workload Management* (SA22-7602).
3. Define RRS as a subsystem.

   Place the following statement in an active IEFSSNxx parmlib member:

   ```
   SUBSYS SUBNAME(RRS)
   ```

   Place this statement after the statement that defines the primary subsystem. The subsystem name (RRS) must match the name of the RRS cataloged procedure. For more information about IEFSSNxx, see *z/OS MVS Initialization and Tuning Reference* (SA22-7592).

   Note: RRS does not support dynamic subsystem definition, so you cannot use the SETSSI ADD,SUBNAME=RRS command to define RRS as a subsystem. Even though this command will appear to succeed, subsequent attempts to start RRS will fail.
4. Set up the RRS log streams.
   •
5. Start RRS.
   - To start RRS with a specific log group name *"lgname"*, enter the following MVS console command:

     ```
     START RRS,GNAME=lgname
     ```
   - To stop RRS, enter the following MVS console command:

     ```
     SETRRS CANCEL
     ```

     Note: Do not stop RRS while WebSphere Application Server for z/OS servers are running.

What to do next

For more information on setting up and running RRS, see *z/OS MVS Programming: Resource Recovery* (SA22-7616).

Preparing the security server (RACF)

About this task

WebSphere Application Server for z/OS uses a SAF-compliant security product for its operating system security interfaces. The WebSphere Application Server for z/OS documentation assumes the use of z/OS Security Server (RACF). If you use another security product, consult the vendor for more information.

All z/OS systems in a sysplex must have access to consistent security information--shared RACF database or equivalent. If a shared security database is not used, you are responsible for ensuring that all WebSphere Application Server for z/OS security definitions are in effect on all systems in the sysplex.

1. Determine which RACF databases provide security information on your z/OS systems. If any WebSphere Application Server for z/OS cell will run on z/OS systems that have no shared RACF database, make plans to guarantee security database consistency for WebSphere Application Server for z/OS user IDs and privileges.
2. WebSphere Application Server for z/OS requires list-of-groups (GRPLIST) checking. This checking is activated by the WebSphere Application Server for z/OS customization jobs. See *z/OS Security Server RACF Security Administrators Guide* for information about GRPLIST support.
3. In order for RACF to automatically select an unused UID or GID value for WebSphere Application Server User IDs and groups:
   a. RACF needs to be using application identity mapping at stage 2 or higher. Use the RACF utility IRRIRA00 to upgrade your security database to application identity mapping stage 2 if necessary.
   b. The RACF profile SHARED.IDS must be defined.
   c. The RACF profile BPX.NEXT.USER must be defined and used to indicate the ranges from which UID and GID values are to be selected.

   For more information, consult the *z/OS Security Server RACF System Programmer's Guide (SA22-7861)* chapter 7, *RACF database utilities*, and the *z/OS Security Server RACF Security Administrator's Guide (SA22-7683)* chapter 20, *RACF and z/OSUnix*.

Preparing TCP/IP

About this task

WebSphere Application Server for z/OS follows the CORBA standard, Internet Inter-ORB Protocol (IIOP), for communications. Accordingly, you must consider changes to your TCP/IP network and modify the TCP/IP configuration.

This section provides background information about changes you will need to make to your Domain Name Server (DNS) and TCP/IP. The actual steps to perform are in the customized instructions of the Profile Management Tool and the zpmt command .

Consider the following tips for your TCP/IP network on z/OS.

- You can get started with a simple Domain Name Server (DNS) name server and a single z/OS image, but you should design your initial configuration with growth in mind.

  You might, for instance, intend to expand your business applications beyond the monoplex to a full sysplex configuration for performance reasons or to prevent a single point of failure. Several considerations come to bear here.

Several DNS implementations and network router implementations allow the use of a generic location service daemon IP name while dynamically routing network traffic to like-configured servers. If you intend to expand your system beyond a monoplex, it might be worthwhile to use one of these implementations from the start. Non-round-robin DNS name servers limit your ability to expand without retrofitting a name server that allows dynamic network traffic routing.

Recommendation: If you are running in a sysplex, set up your TCP/IP network with Sysplex Distributor. This makes use of dynamic virtual IP addresses (DVIPAs), which increase availability and aid in workload balancing.

Beyond Sysplex Distributor, you have your choice of the following DNS and router implementations on or off z/OS:

- Non-round-robin DNS name servers.
- Round-robin DNS name servers.
- Network routers, such as the IBM Load Balancer. (In previous releases, IBM Load Balancer was known as Network Dispatcher.)

- Select the location service daemon IP name.

  For your standalone application server, choose the host name of the server under which you are running. For your deployment manager, choose a generic IP name that can resolve to any or all of the systems where location service daemons run.

  You must define the location service daemon host IP name during installation and customization. Use the location service daemon IP name you chose.

  Note: The administrative console has a location service daemon configuration page on which you set location service daemon variables.

- Select the port for the location service daemon server.

  If you change the location service daemon port number, you can access existing objects after you recycle all your servers. You cannot, however, access the following:

  - Any object handles your application stored to disk
  - Any object references your application stored in the persistent contexts of the name space.

- Set location service daemon port numbers and IP addresses.

  These are initially set using the Profile Management Tool or zpmt command, but you can subsequently change them in the administrative console. Access the location service daemon configuration page through the administrative console navigation bar (on the left side of screen) under System Administration. If you need to use the IIOP through a firewall, ensure that your firewall supports IIOP.

  When recovering a server somewhere other than its configured system, ensure that the same port is not already in use on the system on which it is recovering. If it is, configure the server with a unique port to avoid a conflict.

  If comparing WebSphere Application Server for z/OS and WebSphere Application Server for other platforms, realize that only WebSphere Application Server for z/OS has an ORB SSL port.

  HTTP and HTTPS ports are found in individual servers under the Web container transports, which are in the administrative console as additional properties on the Web container configuration page (which is off the server configuration page).

  Watch for HTTP transport port conflicts if you previously installed WebSphere Application Server for z/OS.

  Ensure that you set up the following port assignments (along with those in the z/OS port assignments chart) on servers that require them in the administrative console:

  - ORB port
  - ORB SSL port
  - Web container transport port
  - Web container transport SSL port

See the administrative console and the information center for more information on the WebSphere variables and how to set their values.

You define ports differently depending on whether they are for the first server or subsequent servers. The first server you create is defined, along with its ports, through the Profile Management Tool or the zpmt command. You have the ability to explicitly specify the ports as you define the server. Subsequent servers and their ports are defined through the administrative console. This means that you define the server first and the ports are automatically assigned. Then, once defined, you can inspect and change the port definitions through the administrative console.

- Some ports, such as the ORB SSL port and the server startup status port, are obtained dynamically.
- Other TCP/IP-related activities include setting up NFS, Web server, and Kerberos (which are all optional).
- If you use the DNS on z/OS, you might want to change the refresh timer interval (-t value) associated with the named location service daemon.

  The -t value specifies the time (nn, in seconds) between refreshes of cell names and addresses and of the weights associated with those names and addresses. The default is sixty seconds. Reducing the -t value will shorten the lapse time required to register the location service daemon IP name with the DNS, but will also increase DNS processing overhead. In our testing, we used an interval of 10 seconds.

  If you use the z/OS DNS, you have to set a location service daemon variable. Do this by setting WebSphere Variable at cell level:

  ```
  daemon_wlmable=1
  ```

  Note: You can perform this for only one cell in a sysplex at a time.

  For details, see *z/OS Communications Server: IP Configuration Reference*.

Checklist: Preparing the base operating system

Print out this worksheet and use it when collecting information about the z/OS system on which you plan to implement WebSphere Application Server for z/OS. Check off each item as you complete the task.

Date: _____

System name: _____ Sysplex name: _____

Preparing z/OS

- _____ Target system hardware and software requirements, including required maintenance in Preventive Service Planning (PSP) bucket, are met.
- _____ UNIX System Services is active with minimum required BPXPRMxx values or better.
- _____ The /tmp directory has at least 20 MB of free space.
- _____ The full dataset names of required system datasets are specified:

Item	Dataset name	In LPA or link list?
SCEERUN		
SCEERUN2		
SIEALNKE		
SCLBDLL2		

- _____ System exits (IEFUSI) do not restrict WebSphere Application Server for z/OS address spaces to less than 512 MB.

- _____ The TSO segment default region size for WebSphere Application Server for z/OS installer and administrator TSO user IDs is at least 128 MB.

Preparing the sysplex

- _____ The target system is configured as a monoplex or into a multisystem sysplex. (Record sysplex name above.)
- _____ System Logger is configured:

Should the application servers reside in a coupling facility **or** DASD-only log streams?	
If a coupling facility, specify the structure name	
SMS data class (for log datasets)	
SMS storage class (for log datasets)	

Preparing JES2 or JES3

- _____ The system proclib for application server cataloged procedures is specified:

System proclib for application server cataloged procedures	

- _____ JES2 exit EXIT06 or JES3 exit IATUX03 do not prevent use of REGION= value on JOB or EXEC statements for WebSphere Application Server for z/OS address spaces.
- _____ Spool space is added if necessary.

Preparing Resource Recovery Services

- _____ The RRS cataloged procedure is present in system proclib:

Procedure name:	

- _____ The RRS dispatching priority is set using SYSSTC or other means.
- _____ The RRS cataloged procedure name is defined as a subsystem name in IEFSSN00. The subsystem name must match the cataloged procedure name.
- _____ The RRS log streams are set up.
- _____ RRS starts successfully.

Preparing Security Server (RACF)

- _____ If multiple security databases are in use, a plan is in place to provide database consistency.

Chapter 8. Planning for product configuration

This tasks helps you plan WebSphere Application Server for z/OS application serving environments for your z/OS target systems.

Before you begin

Complete the steps in Chapter 6, “Installing the product and additional software,” on page 35 and Chapter 7, “Preparing the base operating system,” on page 39.

Read “WebSphere Application Server for z/OS terminology” on page 50.

About this task

WebSphere Application Server for z/OS uses ″application serving environments″ to provide its functions. Configuring these application serving environments after product installation requires a fair amount of planning and coordination. If you have not previously configured WebSphere Application Server for z/OS, you should configure a ″practice″ standalone application server using the default options then proceed to configure the actual product configuration that you want.

Note: On other platforms, the configuration files associated with a WebSphere Application Server runtime environment are called *profiles*; profiles can be copied and manipulated with the manageprofiles command.

In WebSphere Application Server for z/OS, all runtime environments are created with the Profile Management Tool or zpmt command using a profile name of ″default.″ The manageprofiles command and the -profile option on other administrative commands are not used with WebSphere Application Server for z/OS.

Perform the tasks in this section to choose an application serving environment configuration and plan the necessary details for configuration.

1. Decide whether to set up a standalone application server or a Network Deployment cell. See “Standalone and Network Deployment configuration differences” on page 66 for more information.
2. Familiarize yourself with “Considerations for WebSphere Application Server for z/OS” on page 53.
3. (Optional) If you have never set up a WebSphere Application Server for z/OS application serving environment before, follow the steps in “Building a practice WebSphere Application Server for z/OS cell” on page 84 to gain experience in configuring and working with an application serving environment.
4. Follow the directions for the type of application serving environment you want to configure:
   - “Planning for a standalone application server cell” on page 86
   - “Planning for an administrative agent” on page 115.
   - “Planning for a Network Deployment cell” on page 133.
   - “Planning for a new managed node in a Network Deployment cell” on page 157
   - “Planning to federate a standalone server into a Network Deployment cell” on page 180
   - “Planning for a Network Deployment cell with an application server” on page 189
   - “Planning for a secure proxy server” on page 243
   - “Planning for a secure proxy administrative agent” on page 259
   - “Planning for a job manager” on page 224.

   Use the worksheet included with each option to record your planning decisions and additional configuration information.

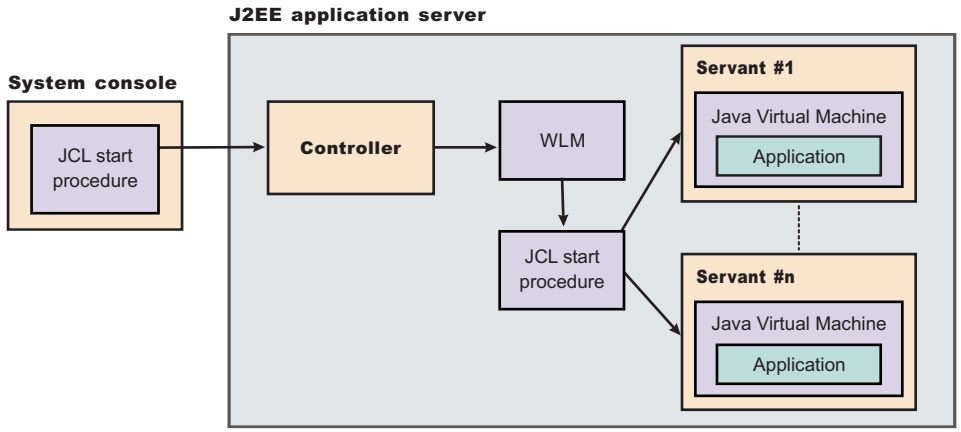
What to do next

When you have completed the planning worksheet for the configuration you have selected, you are ready to configure the application serving environment. See Chapter 9, “Configuring the WebSphere Application Server for z/OS product after installation,” on page 285 for information.

WebSphere Application Server for z/OS terminology

This article covers the different server types on your system as well as other terminology used.

In WebSphere Application Server for z/OS, the functional component on which applications run is called a *server*. Servers comprise address spaces that actually run code.



Within each server are two kinds of address spaces: controllers and servants. A *controller* runs system authorized programs and manages tasks, such as communication, for the server. Each server has one controller that you start with a JCL start procedure when you enter the appropriate start command on the MVS console.

A *servant* is the address space in which the JVM resides. It runs unauthorized programs such as business applications. Depending on the workload, a server has one or more servants running at a time. When work builds up, WLM dynamically starts additional servants to meet the demand.

Note: The location service daemon and node agent are specialized servers and have no servants. The control region adjunct (not shown in the diagrams) is a specialized servant that interfaces with the new service integration busses to provide messaging services.

Here is a quick breakdown of the different server types on your system:

Unmanaged (standalone) application server
The application server that was set up during standalone configuration that hosts your J2EE applications.

Managed (Network Deployment) application server
The application server set up during Network Deployment configuration that hosts your J2EE applications.

Location service daemon
A server that is the initial point of contact for client requests in either configuration.

JMS server
Hosts the JMS function in the WebSphere Application Server for z/OS, which controls the MQ broker and queue manager in either configuration. The JMS server no longer exists as in previous versions of WebSphere Application Server for z/OS. Its function has been replaced with new service integration busses.

Deployment manager
A specialized application server that hosts the administrative console application (it hosts only administrative applications) and provides cell-level administrative function in a Network Deployment configuration. The administrative console application administers servers (grouped into nodes) on many different systems. The deployment manager is the sole occupant of its own node structure that does not need a node agent because there are no application servers in the node, and a cell can have only one deployment manager.

Note: The version of the administrative console application that runs in the deployment manager is designed to manage multinode environments, whereas the version in the standalone application server is for single node environments only.

Node agent
Provides node-level administrative function in a Network Deployment configuration.

Note: Every element of the configuration (servers, clusters, nodes and cells) has both a long and short name:

- The ″Server name″ is the server long name used in the HFS path and the principal name by which the server is known to WebSphere Application Server for z/OS. It is used to identify the server through the administrative console and scripting. It is a mixed case name and greater than 8 characters in length.
- The ″Server short name″ is the platform-specific native alias and the principal name by which the server is known to z/OS. It is used to identify the server to underlying z/OS facilities, such as the Security Server, JES, WLM and ARM. For example, the server short name is used as the MVS JOBNAME.
- The ″Cluster short name″ is used as the WLM application environment name.

A *cluster* is a *logical grouping* of like-configured servers. Clusters exist to promote scalability and availability; workload balancing occurs across the servers in a cluster. Clusters allow you to partition workloads into separate servers while still referring to them as a single unit. Clustering is typically applied to a multinode cell, where each node is configured on a separate system and the cluster has a member (server) on each node. Client requests are distributed among the cluster members based on workload manager decisions.

Note: If you intend for your cluster to span multiple systems in a sysplex, you might need to set up a shared HFS.

A node contains servers that can be part of a cluster. The cluster can span nodes if all involved nodes are in the same cell.

Here is a quick breakdown of cells, nodes, and clusters:

cell A logical collection of WebSphere Application Server for z/OS nodes that are administered together. The cell is the largest unit of organization.

- Nodes that comprise a cell can reside on systems in the same sysplex, differing sysplexes, on the same z/OS monoplex, or on differing systems entirely. A cell that consists of nodes on differing systems or sysplexes is called a *heteregeneous cell*.
- A z/OS sysplex or monoplex can contain multiple WebSphere Application Server for z/OS cells.
- Different cells can have nodes on the same systems, although a given node can be a member of only one cell.

- There are two kinds of WebSphere Application Server for z/OS cells: standalone application servers and Network Deployment cells.

node A logical collection of servers on a particular z/OS system in the cell.

- The cell to which a node belongs can span several systems, but the node must remain within a single z/OS system.
- A z/OS system can contain multiple WebSphere Application Server for z/OS nodes, belonging to the same or different cells.
- A standalone WebSphere Application Server for z/OS cell consists of a single node. Due to administrative constraints, this node should have only a single application server in it.
- A Network Deployment cell consists of a deployment manager node, which is responsible for cell-wide administrative tasks, and any number of federated nodes. Each federated node contains a node agent, which handles communication with the cell's deployment manager, and any number of application servers.

cluster

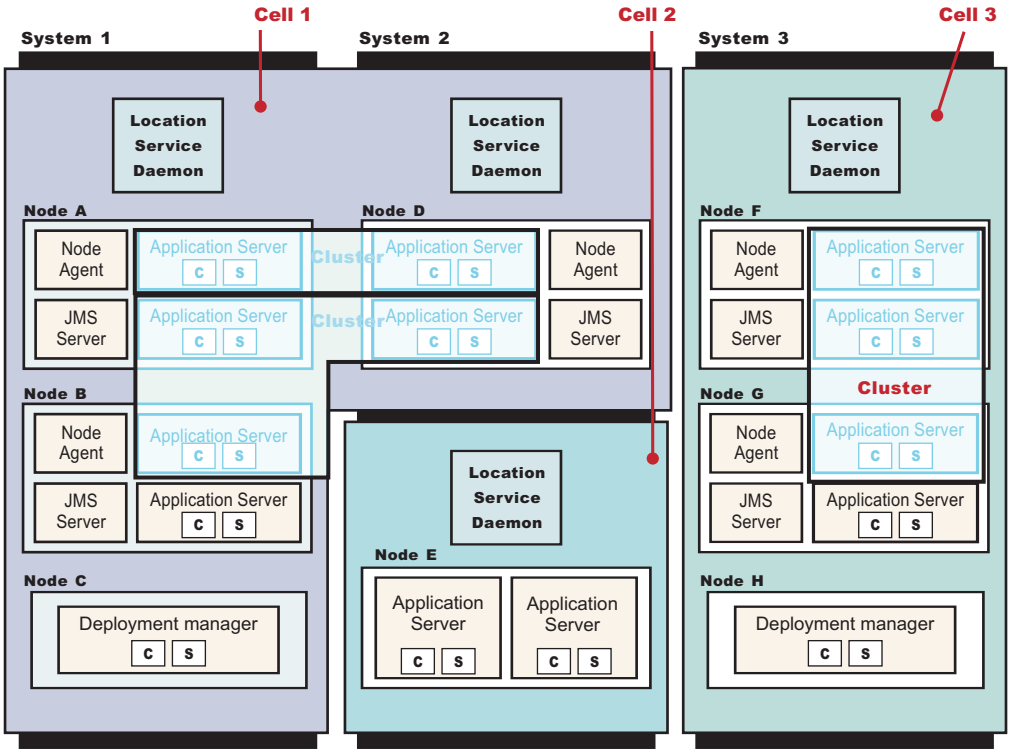
A logical collection of like-configured application servers that provides performance, reliability and administration advantages.

- A cluster can span nodes and systems within the same cell.
- Clusters are not a layer in the cell/node/server hierarchy. Instead, they are a way of grouping servers that host the same applications within a cell.

A cluster can span nodes and systems within the same cell.

To help you understand the interaction between servers, clusters, nodes and cells, here is a diagram depicting various configurations you can set up in your Network Deployment sysplex:

WebSphere for z/OS: Possible configurations in a sysplex



Cells 1 and 3 in the illustration depict Network Deployment configuration cells. Cell 2 is a standalone configuration cell.

Note: This precise node assignment does not need to apply. The deployment manager node can exist on one system, other nodes that have been federated into the deployment manager can exist on differing systems. Such a configured cell of differing machines or operating systems is called a *heterogeneous cell* and expands the possible topologies you can consider for your network deployment.

Using a heterogeneous cell to support mixed platforms within a cell

With careful planning, you can manage cells across different z/OS Sysplex and different operating systems.

Cells can span z/OS sysplex environments and spanning other operating systems. For example, z/OS nodes, Linux nodes, UNIX nodes, and Windows nodes can exist in the same Application Server cell. This kind of configuration is referred to as a *heterogeneous* cell.

A heterogeneous cell does require significant planning. The Heterogeneous Cells – cells with nodes on mixed operating system platforms white paper outlines the planning and system considerations required to build a heterogeneous cell.

Related tasks

"Preparing the sysplex" on page 41

Considerations for WebSphere Application Server for z/OS

Familiarize yourself with the z/OS facilities used by the WebSphere Application Server for z/OS application serving environment.

Digital certificates and key rings or key stores are required for Secure Socket Layer communication. These certificates may be stored in the System Authorization Facility (SAF) security database, or in files in the configuration file system.

System Authorization Facility profiles are created during customization to grant necessary authorities to WebSphere Application Server for z/OS address spaces.

Component Trace (CTRACE) facilities in WebSphere Application Server for z/OS are used to manage the collection and storage of trace data. CTRACE data is written to address space buffers in private (pageable) storage, which can be formatted using IPCS if a dump of the address space is taken. CTRACE data can also be written to trace datasets on disk or tape using an external writer. Although CTRACE data is primarily output for use by IBM service personnel, using CTRACE capabilities at your installation allows you to have additional trace data available when a problem first occurs. Because CTRACE efficiently uses system resources, you can collect valuable trace data with minimal impact on performance.

System Logger is used by WebSphere Application Server for z/OS. This is an MVS component that allows applications to log data in a sysplex, to log error and trace information and provide XA transaction logging. The System logger creates and manages log streams, which are written first to a coupling facility or local in-memory buffer, then transferred to log datasets on DASD for longer term access. Log streams that are written to local buffers rather than to a coupling facility are called DASD-only log streams.

System Authorization Facility groups are used by WebSphere Application Server for z/OS to associate user IDs with common sets of permissions.

A common set of SAF groups is used across a WebSphere Application Server for z/OS cell.

A **System Authorization Facility user ID** is associated with each WebSphere Application Server for z/OS address space. (A SAF-compliant security package, such as RACF, is required by the WebSphere Application Server runtime.)

Cataloged procedures

This concept is an explanation of how WebSphere Application Server for z/OS server uses the JCL cataloged procedures.

Each WebSphere Application Server for z/OS server uses a JCL cataloged procedure. These procedures are all fairly similar and consist of a main cataloged procedure and an INCLUDE member that contains DD statements. Here are sample cataloged procedure library members for a controller as generated by the Profile Management Tool or the zpmt command:

Procedure library member BBO7ACR:

```
//BBO7ACR  PROC ENV=,PARMS=' ',REC=N,AMODE=00
// SET ROOT='/wasv7config/bbobase/bbonode'
// SET FOUT='properties/service/logs/applyPTF.out'
// SET WSDIR='AppServer'
//*************************************************************
//* Test that OMVS can successfully launch a shell and return *
//*************************************************************
//TOMVS   EXEC PGM=BPXBATCH,REGION=0M,
// PARM='SH exit 13'
//STDOUT   DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWXG)
//STDERR   DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWXG)
//*********************************************************
//* If the shell RC code is as expected (13) - proceed    *
//*********************************************************
//IFTST   IF (RC = 13) THEN
//*********************************************************
//* Start the Multi-Product PTF Post-Installer            *
//*********************************************************
//APPLY   EXEC PGM=BPXBATCH,REGION=0M,
// PARM='SH &ROOT./&ENV..HOME/bin/applyPTF.sh inline'
//STDOUT   DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWXG)
//STDERR   DD PATH='&ROOT./&ENV..HOME/&FOUT.',
// PATHOPTS=(OWRONLY,OCREAT,OAPPEND),PATHMODE=(SIRWXU,SIRWXG)
//       IF (APPLY.RC <= 4) THEN
//*********************************************************
//* If the RC from the Post-Installer is LE 4 then start  *
//* the WebSphere Application Server                      *
//*********************************************************
//STEP1    EXEC PGM=BPXBATA2,REGION=0M,TIME=MAXIMUM,MEMLIMIT=NOLIMIT,
// PARM='PGM &ROOT./&WSDIR./lib/bbooctlm &AMODE. &PARMS. REC=&REC'
//STDENV DD PATH='&ROOT/&ENV/was.env'
//*
//* Output DDs
//*
//CEEDUMP   DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//STDOUT    DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//STDERR    DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//DEFALTDD  DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//HRDCPYDD  DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//          ENDIF
//IFTSTEND ENDIF
```

Procedure library member BBO7ASR:

```
//BBO7ASR  PROC ENV=,AMODE=00
//  SET ROOT='/wasv7config/bbobase/bbonode'
//  SET WSDIR='AppServer'
//STEP1   EXEC PGM=BPXBATSL,REGION=0M,TIME=NOLIMIT,MEMLIMIT=NOLIMIT,
//         PARM='PGM &ROOT./&WSDIR./lib/bboosrmr &AMODE.'
//STDENV    DD PATH='&ROOT/&ENV/was.env'
//*
```

```
//* Output DDs
//*
//CEEDUMP   DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//STDOUT    DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//STDERR    DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//DEFALTDD  DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
//HRDCPYDD  DD SYSOUT=*,SPIN=UNALLOC,FREE=CLOSE
```

The PGM=parameter passed to the shell program BPXBATA2 on the EXEC statement in the cataloged procedure specifies the type of WebSphere Application Server for z/OS server. The program names are as follows:

- bbooctlm (controller)
- bboosrmr (servant)
- bboocram (adjunct process)
- bbodmnm (location service daemon)

The PARM= parameter on the EXEC PGM statement contains the parameters that are passed to the program identified by the PGM= parameter.

Note: The appropriate interface for making changes to the language environment (LE) parameters is through the was.env file; however, do not modify any LE parameters without first consulting with the IBM Software Support team. The LE parameters are set internally to ensure the best possible performance of the WebSphere Application Server, which is the main LE application running in the address space. If you need to add or change LE parameters, make sure that you work with the IBM Software Support team to ensure that the internally set parameters are not compromised.

The STDENV DD statement points to the was.env (startup parameter) file for the server. The path to this file consists of the configuration HFS directory name (hardcoded using the ROOT JCL variable) and the symbolic link for this particular server, which is specified at startup using the ENV= parameter.

The controller cataloged procedure includes some additional statements before the EXEC statement that invokes BPXBATA2. These are used to invoke the post installer program that applies any needed maintenance to the configuration HFS and its home directories when service is applied to the product HFS and load modules.

The following sections describe the cataloged procedures required for each configuration, provide a recommended naming convention, and explain how the SAF user ID for each server is determined.

Cataloged procedures for standalone application servers

A standalone application server uses the following cataloged procedures:

- Controller cataloged procedure
- Servant cataloged procedure
- Adjunct process cataloged procedure
- Location service daemon cataloged procedure

You can use the same cataloged procedures for different standalone servers if the configuration HFS and product code level (including STEPLIB) are the same for both servers.

Cataloged procedures for Network Deployment cells

A Network Deployment cell uses the following cataloged procedures:

For the deployment manager:

- Deployment manager controller cataloged procedure

- Deployment manager servant cataloged procedure

For each application server node:
- Application server controller cataloged procedure (also used for the node agent)
- Application server servant cataloged procedure

For the location service daemon (one per z/OS system):
- Location service daemon cataloged procedure

The application server servant cataloged procedure is the only one likely to require modification, in order to place libraries (CICS, DB2, and so on) in the STEPLIB concatenation.

You can use the same cataloged procedures for several nodes in a Network Deployment cell, or even for several cells, if the configuration HFS is the same for all of them.

A recommended cataloged procedure naming convention

Use a consistent naming convention for your WebSphere Application Server for z/OS cataloged procedures. The procedure name should distinguish between WebSphere Application Server for z/OS version and configuration HFS

The following convention works for either a standalone application server or Network Deployment cell, for example, where *cc* is a two-character cell identifier:

Deployment manager controller	*cc*7DCR
Deployment manager servant	*cc*7DSR
Location service daemon controller	*cc*7DMN
Application server controller	*cc*7ACR
Application server servant	*cc*7ASR
Control region adjunct	*cc*7AAR

If you require separate cataloged procedures for nodes on different systems in a sysplex (if they need independently settable STEPLIB statements to allow for a nondisruptive restart for example), either place the location service daemon and application server procedures in system-specific proclibs or append a one-character system identifier to the cataloged procedure names for the location service daemon and application servers.

Assigning user IDs to WebSphere Application Server for z/OS address spaces

If you use z/OS Security Server (RACF) as your SAF-compliant security system on z/OS, then STARTED class profiles are used to assign started task user IDs to each WebSphere Application Server for z/OS server. These STARTED profiles are set up by the batch jobs created by the Profile Management Tool or the zpmt command. Update these STARTED profiles as needed to place servers that you create yourself under the appropriate user IDs.

Controllers (deployment manager, location service daemon, node agent or applications server controller) are started using a console `START` command that you issue either from the MVS console or internally. For these servers, the STARTED profile name that is checked is of the form *procname*.*jobname*.

Whenever it creates a controller or daemon cataloged procedure, the Profile Management Tool or the zpmt command also creates a STARTED profile that associates all controllers using that cataloged procedure with the appropriate controller user ID and configuration group. If you set up a standalone application server with default names, therefore, the Profile Management Tool or the zpmt command would create the following STARTED profiles for controllers:
- `RDEFINE STARTED BBO7ACR.* STDATA(USER(WSCRU1) GROUP(WSCFG1) TRACE(YES))`
- `RDEFINE STARTED BBO7DMN.* STDATA(USER(WSCRU1) GROUP(WSCFG1) TRACE(YES))`

Note: TRACE(YES) writes message IRR812I to the MVS console whenever the profile is used.

Servant regions (application server servants and adjunct processes) are started using Workload Manager (WLM). For these servers, the STARTED profile name that is checked is of the form *jobname*.*jobname*.

Unfortunately, there is no way to assign all servers using a particular servant cataloged procedure to a servant user ID. Therefore, the Profile Management Tool or the zpmt command creates a STARTED profile for each servant and one for each control region adjunct. If default names are chosen, the following servant STARTED profiles are created for a standalone application server:

- RDEFINE STARTED BBOS001S.* STDATA(USER(WSSRU1) GROUP(WSCFG1) TRACE(YES))
- RDEFINE STARTED BBOS001A.* STDATA(USER(WSCRU1) GROUP(WSCFG1) TRACE(YES))

When you choose cataloged procedure names, make sure that the appropriate STARTED profile is in place to map the server to its appropriate SAF user ID. Use the RACF ISPF panels or the RLIST STARTED command to display the STARTED profiles.

If you use another SAF-compliant security system, contact the security server vendor for WebSphere Application Server for z/OS setup information.

Cataloged procedure for the administrative asynchronous task

The asynchronous administrative task also requires a cataloged procedure. This very simply cataloged procedure does not include a STEPLIB or configuration HFS pointer. Because it must run under a specific user ID and group associated with the security domain of the cell for which it runs, however, you must choose a different cataloged procedure name for each security domain or cell.

Note: Name the administrative asynchronous task cataloged procedure "*cc*ADMH," where *cc* is a two-character cell identifier.

Configuration file system

There are several planning decisions that you need to make when setting up a WebSphere Application Server for z/OS configuration file system.

Cell, node, and server settings as well as deployed applications are stored in the WebSphere Application Server for z/OS configuration file system.

Note: You can use a zSeries file system (ZFS) or hierarchical file system (HFS) for the configuration file system.

Note: Beginning with WebSphere Application Server for z/OS Version 7.0, the SBBOLOAD and SBBOLD2 datasets no longer exist by default. This is because the load modules are now in the file system. If you want to switch a configuration from using load modules in the file system to using load modules in a dataset, you can use the tool described in “switchModules command” on page 383.

Each node needs a home directory

Every WebSphere Application Server for z/OS node--whether a standalone application server, deployment manager, managed application server node, or location service daemon--requires a read/write home directory, sometimes referred to as its WAS_HOME.

This is the structure of a WebSphere Application Server for z/OS configuration file system, mounted at /WebSphere/V7R0. It contains a WebSphere Application Server home directory for a single application server named BBOS001, with a cell and a node both named SYSA.

```
/WebSphere/V7R0
  /AppServer
    /bin
    /classes
    /java
    /lib
    /logs
    /profiles
    /default -> this is the profile_root directory
    /temp
    ...
   /Daemon
    /config
      /SYSA
   SYSA.SYSA.BBODMNB -> /WebSphere/V7R0/Daemon/config/SYSA/SYSA/BBODMNB
   SYSA.SYSA.BBOS001 ->
/WebSphere/V7R0/AppServer/profiles/default/config/cells/SYSA/nodes/SYSA
   /servers/server1
   SYSA.SYSA.BBOS001.HOME ->  /WebSphere/V7R0/AppServer
```

The WebSphere Application Server home directory for BBOS001 is named AppServer. It contains directories with complete configuration information for the SYSA node and the BBOS001 server.

The /Daemon directory contains configuration information for location service daemons defined to nodes in this configuration file system.

Note: The /Daemon/config subdirectory is subdivided by cell name. If the cells have different short names, the location service daemon information for each is kept separate.
The daemon home directory has the fixed WebSphere Application Server home name *Daemon*.

Symbolic links are used to access startup parameters

In addition to the WebSphere Application Server home directories themselves, the configuration file system contains a multipart symbolic link for each server that points to the startup parameters for the server. The symbolic link is named *cell_short_name.node_short_name.server_short_name*.

The sample configuration file system above contains a symbolic link SYSA.SYSA.BBODMNB to start the location service daemon and a symbolic link SYSA.SYSA.BBOS001 to start the BBOS001 application server. The second symbolic link is specified in the ENV parameter on the `START` command when the server or location service daemon is started from the MVS console:

```
START procname,JOBNAME=BBOS001,ENV=SYSA.SYSA.BBOS001
```

Each symbolic link points to the subdirectory where the server's was.env file resides. This file contains the information required to start the server.

Note: During post-installation processing, described below, the server JCL needs to specify the WebSphere Application Server home directory itself, rather than the location of the was.env file. This is the purpose of the SYSA.SYSA.BBOS001.HOME symbolic link shown above.

Sharing the configuration file system between cells

Two or more WebSphere Application Server for z/OS cells (standalone application server, Network Deployment, or both) can share a WebSphere Application Server for z/OS configuration file system, provided the following conditions are met:

- All cells using the configuration file system must be set up using the same common groups and users. In particular, each must have the same administrator user ID and configuration group.
- The cells must have distinct cell short names.

- Each node must have its own WAS_HOME directory that is not shared with any other node or cell.

As noted above, you can share the daemon home directory (/Daemon) between cells, as it has subdirectories farther down for each cell in the configuration file system.

Note: Be aware that sharing a configuration file system between cells increases the likelihood that problems with one cell might cause problems with other cells in the same configurations file system.

Sharing the configuration file system between systems

Two or more z/OS systems can share a configuration file system, provided the z/OS systems have a shared file system and the configuration file system is mounted R/W. All updates are made by the z/OS system that ″owns″ the mount point. For a Network Deployment cell, this is generally the z/OS system on which the cell deployment manager is configured.

Choosing a WebSphere Application Server for z/OS configuration file system mount point

The choice of WebSphere Application Server for z/OS configuration file system mount points depends on your z/OS system layout, the nature of the application serving environments involved, and the relative importance of several factors: ease of setup, ease of maintenance, performance, recoverability, and the need for continuous availability.

In a single z/OS system:

If you run WebSphere Application Server for z/OS on a single z/OS system, you have a wide range of choices for a z/OS configuration file system mount point. You might want to put several standalone application servers in a single configuration file system with a separate configuration file system for a production server or for a Network Deployment cell. Using separate configuration file system datasets improves performance and reliability, while using a shared configuration file system reduces the number of application server cataloged procedures you need.

You might have one configuration file system with your development, test and quality assurance servers, all in the same common groups and uses as in the following example:

```
/WebSphere/V7_test
  /DevServer - home to standalone server DVCELL, with server DVSR01A
  /TestServer1 - home to standalone server cell T1CELL, with server T1SR01A
  /TestServer2 - home to standalone server cell T2CELL, with server T2SR01A
  /QAServer - home to Network Deployment cell QACELL, with deployment
    manager QADMGR and server QVSR01A
```

and a separate configuration HFS for your production cell:

```
/WebSphere/V7_prod
  /CorpServer1 - home to Network Deployment cell CSCELL, with deployment
    manager CSDMGR and server CSSR01A
```

In a multisystem z/OS sysplex with no shared HFS:

In a multisystem sysplex with no shared HFS, each z/OS system must have its own configuration file system datasets. For standalone application servers and for Network Deployment cells that do not span systems, the options are the same as for a single z/OS system.

For Network Deployment cells that span systems:

Here you have two options:

- You can use a different mount point for the cell's configuration file system datasets on each system. This allows you to move nodes easily between systems (if a system becomes inoperative or is being

upgraded for example), since each mount point is unused on the other systems in the sysplex, allowing you to mount the failed system's configuration file system datasets on an alternate system in the sysplex.

On system LPAR1, for example, you might have a configuration file system for one part of a cell:

```
/var/WebSphere/V7config1
  /DeploymentManager - home to deployment manager F1DMGR in cell F1CELL
  /AppServer1 - home to node F1NODEA and servers F1SR01A and F1SR02A
```

with a second configuration file system on LPAR2:

```
/var/WebSphere/V7config2
  /AppServer2 - home to node F1NODEB and servers F1SR02B (clustered)
    and F1SR03B
```

This setup has the advantage that you can move the deployment manager and node F1NODEA to LPAR2 or move node F1NODEB to LPAR1. The disadvantage of this configuration is that F1NODEA and F1NODEB will require separate sets of cataloged procedures.

- Or you can use the same mount point for all configuration file system datasets in a particular cell. This allows you to use common cataloged procedures and make the systems look very similar.

  Using the same cell setup as above, node LPAR1 would have one configuration file system:

  ```
  /var/WebSphere/V7F1
    /DeploymentManager - home to deployment manager F1DMGR in cell F1CELL
    /AppServer1 - home to node F1NODEA and servers F1SR01A and F1SR02A
  ```

  and LPAR2 would have a separate file system at the same mount point:

  ```
  /var/WebSphere/V7F1
    /AppServer2 - home to node F1NODEB and servers F1SR02B (clustered)
      and F1SR03B
  ```

  However, relocation of either LPAR's node(s) to the other system would require merging a copy of one configuration file system into the other.

In a multisystem z/OS sysplex with a shared HFS:

If your sysplex has a shared hierarchical file system, you can simply mount a large configuration file system for the entire cell. When using the Profile Management Tool or the zpmt command, specify the common configuration file system mount point on each system. As noted above, you should update the configuration file system from the z/OS system hosting the deployment manager. Performance will depend on the frequency of configuration changes, and ensure you devote extra effort to tuning if this option is chosen.

Alternatively, you can mount a separate configuration file system on each system, perhaps using the system-specific file system mounted at /&SYSNAME on each system:

```
/LPAR1/WebSphere/V7F1
  /DeploymentManager - home to deployment manager F1DMGR in cell F1CELL
  /AppServer1 - home to node F1NODEA and servers F1SR01A and F1SR02A

/LPAR2/WebSphere/V7F1
  /AppServer2 - home to node F1NODEB and servers F1SR02B (clustered)
    and F1SR03B
```

Each system (LPAR1 and LPAR2) mounts its own configuration file system on its system-specific mount point. When using the Profile Management Tool or the zpmt command, specify the following:

- /LPAR1/WebSphere/V7F1 on LPAR1
- /LPAR2/WebSphere/V7F1 on LPAR2

Performance is better with this option than with a shared sysplex, and, depending on choice of mount point, it might be possible to mount a configuration file system temporarily on the other LPAR if the original owner is down. You can make cataloged procedures system-specific or use &SYSNAME to select the configuration file system mount point.

If you really want to use the same apparent mount point for all configuration file system datasets, you can use symbolic links to redirect a common mount point to a different file system on each system:

- ln -s $SYSNAME/WebSphere WebSphere
- Mount LPAR1's configuration file system at /LPAR1/WebSphere/V7F1.
- Mount LPAR2's configuration file system at /LPAR2/WebSphere/V7F1.

If this is done correctly, you can specify a configuration mount point of /WebSphere/V7F1 for each system in the Profile Management Tool or the zpmt command and still enjoy the benefits of system-specific customization file system datasets. However, when this setup is used, it is **not** possible to easily move configuration file system datasets from one system to another. All nodes expect to find their data in /WebSphere/V7F1, and you can mount only one configuration file system at this mount point on each system.

Recommendations:

- On a single z/OS system, create a read/write file system at /wasv7config and use the Profile Management Tool defaults, mounting each configuration file system at /wasv7config/*cell_name*/*node_name*.
- On a multisystem sysplex with no shared file system, follow the recommendations above for a single z/OS system. This will allow you to use common cataloged procedures for each cell. Establish separate mount points on each system for any cell that you might need to recover on an alternate system in the sysplex.
- On a multisystem sysplex with a shared file system, use a shared configuration file system when performance is not an issue or when a shared file system is required to support specific WebSphere Application Server for z/OS functions. Use nonshared configuration file system datasets when performance is an issue, or when you must avoid a single point of failure.

Choosing WebSphere Application Server home directory names

The WebSphere Application Server home directory is always relative to the configuration file system in which it resides. In the Profile Management Tool or the zpmt command, therefore, you choose the configuration file system mount point on one panel and fill in just the single directory name for the home directory on another. But when instructions direct you to go to the WAS_HOME directory for a server, they are referring to the entire path name, configuration file system and home directory name combined (/WebSphere/V7R0/AppServer for example).

You can choose any name you want for a home directory if it is unique in the configuration file system. If you are creating a standalone application server or new managed server node to federate into a Network Deployment cell, be sure to choose one that is not in use in the Network Deployment cell's configuration file system.

If you have one node per system, you might want to use some form of the node name or system name. Alternatively, you can use ″DeploymentManager″ for the deployment manager and ″AppServer*n*″ for each application server node.

Relationship between the configuration file system and the product HFS

The configuration file system contains a large number of symbolic links to files in the product HFS (/usr/lpp/zWebSphere/V7R0 by default). This allows the server processes, administrator, and clients to access a consistent WebSphere Application Server for z/OS code base.

Note that these symbolic links are set up when the WebSphere Application Server home directory is created and are very difficult to change. Therefore, systems that require high availability should keep a separate copy of the WebSphere Application Server for z/OS product HFS and product datasets for each maintenance or service level in use (test, assurance, production, and so forth) to allow system maintenance, and use intermediate symbolic links to connect each configuration HFS with its product HFS.

Note: If you configure your Network Deployment environment using the default value for the product HFS path in the Profile Management Tool or the zpmt command, it will result in all the nodes pointing directly at the mount point of the product HFS. This makes rolling maintenance in a nondisruptive manner almost impossible. If a cell is configured in this way, applying service to the product HFS affects all the nodes at the same time; and if multiple cells are configured in this way, applying service to the product HFS affects all the cells at the same time. You might want to specify what is referred to as an ″intermediate symbolic link″ between each node's configuration HFS and the actual mount point of the product HFS. This strategy is described in the WebSphere Application Server for z/OS V5 - Planning for Test, Production and Maintenance white paper. See the WebSphere z/OS V6 -- WSC Sample ND Configuration white paper for more information about this issue and its relationship to applying maintenance. See the WebSphere for z/OS: Updating an Existing Configuration HFS to Use Intermediate Symbolic Links instructions for information on obtaining and using a utility that would allow you to update an existing configuration HFS to use intermediate symbolic links.

When a WebSphere Application Server for z/OS node is started, the service level of the configuration is compared against the service level of the product file system. If the configuration file system service level is higher than that of the product file system (probably meaning that an old product file system is mounted), the node's servers will terminate with an error message. If the configuration file system service level is lower than that of the product file system (meaning that service has been applied to the product code base since the node was last started), a task called the post-installer checks for any actions that need to be performed on the configuration file system to keep it up to date. For more information about the post-installer, see Chapter 10, “Applying product maintenance,” on page 385.

Log streams

The z/OS System Logger provides for collections of data called ″log streams,″ which can be written to local storage buffers or to a sysplex coupling facility and then to DASD for long-term storage. Log streams can provide high-performance logging for certain applications.

For general information about log streams, read *z/OS Setting Up a Sysplex* (SA22-7625).

WebSphere Application Server for z/OS can use log streams for the following two types of data:

- Data in the WebSphere Application Server error log, which can be routed to a log stream instead of to a print dataset
- Data in WebSphere Application Server transaction logs, which can be routed to a log stream instead of to a hierarchical file system (HFS) dataset

WebSphere Application Server error log

The WebSphere Application Server error log is used to record detailed runtime error and status messages. If the ras_log_logstreamName variable is set, error log messages are written to the named z/OS log stream. If the ras_log_logstreamName variable is not set or if the named log stream does not exist, error log records are written to STDERR.

The primary advantage of sending the WebSphere Application Server error log to a z/OS log stream is that you can consolidate error logs from multiple servers and servant regions. If you place the error log stream in a coupling facility, you can also consolidate error logs from different systems in the same sysplex.

WebSphere Application Server for z/OS provides the following sample jobs in the SBBOJCL product dataset to create error log streams:

BBOERRLC
Create a coupling facility log stream for the WebSphere Application Server error log

BBOERRLD
Create a DASD-only log stream for the WebSphere Application Server error log

After you create the log stream, use scripting or the administrative console to set the ras_log_logstreamName variable to the log stream name for all servers whose output is to go to the newly created log stream.

Use the BBORBLOG script in the SBBOEXEC profile dataset to view the error log. Read the ″Viewing error log contents through the Log Browse Utility″ article in the information center for more information.

Transaction XA partner log

The WebSphere Application Server transaction XA partner log is used to record transaction (JTA) information. This information is written to an HFS file or a z/OS log stream, depending on the setting of the transaction directory file for a specific server:

- If the transaction directory value is dir://*directory_name*, the named file system directory is used for storing transaction information.
- If the transaction directory value is logstream://*logstream_name*, transaction information is written to the named log stream.

The default is dir://*app_server_root*/tranlog/*server_name*.

By using a z/OS log stream for the WebSphere Application Server transaction log and placing that log stream in a coupling facility, you can improve performance for cross-system restart operations.

WebSphere Application Server for z/OS provides the following sample jobs in the SBBOJCL product dataset to create transaction log streams:

BBOTXALC
Create a coupling facility log stream for a WebSphere Application Server transaction log

BBOTXALD
Create a DASD-only log stream for a WebSphere Application Server transaction log

After you create the log stream, use the administrative console to set an individual server's transaction log to logstream://*logstream_name* on the configuration tab of the server's transaction service settings (**Servers > Application Servers > *server_name* > Container Services > Transaction Service**) and restart the server. Read the ″Transaction service settings″ article in the information center for more information.

Note: When an application server is federated into a Network Deployment cell, you must clear any existing transaction errors. If transaction logging is being done to a z/OS log stream, delete the server's transaction log stream after the application server is shut down and recreate it before starting the newly federated application server.

Output destinations

Various server DD statements are used to address system output, such as, console output, trace output, and dump output.

Since WebSphere Application Server controllers and servants are z/OS started task address spaces, they can produce a variety of output:

- Server output and error messages
- Trace records
- System dumps.

This output can be written to a variety of destinations:
- JES2 print and punch files (referred to as ″STDERR″ or ″job output″)
- Files written to the configuration file system or other file systems
- z/OS log streams
- Component trace datasets.

Scheduler database

This concept describes the scheduler service in WebSphere Application Server and the timing intervals.

The scheduler service in WebSphere Application Server is responsible for starting actions at particular times or intervals. The performance of the scheduler database is critical to efficient scheduler operation.

WebSphere Application Server for z/OS provides the following sample jobs in the SBBOJCL product dataset to create a local scheduler database using DB2:

BBOCRTTS	Create DB2 table spaces for a scheduler database
BBOCRTSC	Create DB2 schemas for a scheduler database

The following sample jobs in SBBOJCL can be used to delete a scheduler database in DB2 when it is no longer needed:

BBODRPSC	Drop DB2 schemas for a scheduler database
BBODRPTS	Drop DB2 table spaces for a scheduler database

Make copies of these jobs, customize them according to the instructions in the job, and run as needed to create or delete scheduler databases.

TCP/IP port conventions

This article lists the default server values for WebSphere Application Server for z/OS.

z/OS port assignments

The following table lists the default port assignments for z/OS.

Port	Standalone location service daemon	Standalone application server	ND location service daemon	ND application server	Node agent	Deployment manager
HTTP		9080		9080		
HTTP/S		9443		9443		
Admin Console Port	9060			9060		9060
Admin Console Secure Port	9043			9043		9043
Bootstrap		2809		9810	2809	9809

Port	Standalone location service daemon	Standalone application server	ND location service daemon	ND application server	Node agent	Deployment manager
ORB	5655	2809	5755	9810	2809	9809
ORB SSL	5656	0	5756	0	0	0
SOAP/JMX		8880		8880	9360	8879
Node Discovery					7272	
Node Multicast Discovery					5000	
Cell Discovery						7277
Service Integration		7276				
Service Integration Secure		7286				
Service Integration MQ Interoperability		5558				
Service Integration MQ Interoperability Secure		5578				
Session Initiation Protocol Port		5060				
Session Initiation Protocol Secure Port		5061				
High Availability Manager Communications		9353			9354	9352

Location service daemon ports

Standalone application server node location service daemons are considered temporary. The ports assigned to a standalone application server node's location service daemon are used only until that node is federated. It is advisable to set aside a couple of ports to serve as ″interim ports″ for the standalone application server node location service daemon. The ″permanent″ location service daemon ports are the ones assigned to the deployment manager. Those same ports are copied to location service daemons created when a standalone application server node on another MVS image is federated into the deployment manager cell.

Node agent ports

There is a node agent per MVS image on which the cell spans. One design option calls for all node agents to have the exact same ports so the Sysplex Distributor is able to balance the traffic between the

two. The node agent is created when the BBOWADDN customized job is run.

Server clusters

A server cluster is a grouping of two or more servers into a one logical server. A cluster is created through the administrative console. Servers within a cluster are called ″cluster members.″ Servers (″members″) within a cluster start out being clones of one another. When it comes to the TCP ports for the members in a cluster, the administrative console allows you during the creation of the cluster to specify if you want the HTTP ports to be unique or the same. The other ports -- bootstrap, DRS, ORB, ORB SSL and SOAP -- will be made unique by the application server.

For complex configurations with multiple members in a cluster it is advisable to make the members be as nearly identical to one another as possible, including the TCP ports. Therefore, when planning it is recommended a range of ports be allocated for a cluster with the intention to make certain all members of that cluster were given the same set of ports. Because WebSphere will automatically generate unique DRS, ORB, ORB SSL and SOAP ports for the second cluster member, it is necessary to go back in and remap the ports back to the ports set aside for the server cluster

Note: When a ″vertical cluster″, two members on the same MVS image, is the potential configuration, you will need to consider port sharing by two members of the same cluster on the same MVS image.

Related tasks

Chapter 8, “Planning for product configuration,” on page 49
This tasks helps you plan WebSphere Application Server for z/OS application serving environments for your z/OS target systems.

Workload management

This concept is an explanation of how WebSphere Application Server for z/OS uses the workload management (WLM) function of z/OS to start and manage servers in response to workload activity.

Each Java EE application server in a WebSphere Application Server for z/OS cell uses WLM to start servants as WLM application environments. Thus, each application server must be associated with a WLM application environment name. The ″Cluster transition name″ in the WebSphere Application Server for z/OS configuration is used as the WLM application environment name.

Standalone and Network Deployment configuration differences

A table is presented that contains specifics on the differences between a WebSphere Application Server for z/OS standalone cell and Network Deployment cell.

	Standalone cell	Network Deployment cell
Configuration:	Set up each standalone server node through the Profile Management Tool or the zpmt command. Set up additional servers within the node through the administrative console or scripting.	Set up each deployment manager node through the Profile Management Tool or the zpmt command. Add application server nodes to the Network Deployment cell through the Profile Management Tool or the zpmt command.
Address spaces:	Minimum: four (location service daemon, controller, servant, control region adjunct)	Minimum: seven (location service daemon, application server controller, application server servant, application server control region adjunct, deployment manager controller, deployment manager servant, node agent)
	Maximum: Limited only by resources.	Maximum: Limited only by resources.

	Standalone cell	Network Deployment cell
Administrative isolation:	Each standalone server node is a separate administrative domain.	All nodes in the cell are in the same administrative domain.
Operational isolation:	You can start and stop servers independently. Each server has an independent, unshared JNDI namespace.	You can start and stop servers independently. The JNDI namespace is shared among all servers in the cell.
Application servers allowed to have multiple servants?	Yes	Yes
Clustering available?	No	Yes

Application server naming conventions

There are several names that you must specify during WebSphere Application Server for z/OS configuration. Although it is possible to assign names to WebSphere Application Server for z/OS objects on an ad-hoc basis, it is safer and more efficient to assign names in an orderly fashion.

Long names and short names

Each WebSphere Application Server for z/OS cell, node, server, and cluster must have both a long name and a short name.

Long names

Long names are the principal names by which cells, nodes, servers, and clusters are known to WebSphere Application Server for z/OS. These are the names used in scripting and the administrative console. Long names can be up to 50 characters long and include mixed-case alphabetic characters, numeric characters, and the following special characters: ! ^ ( ) _ - . { } [ ]

Short names

Short names are specific to the z/OS implementation of WebSphere Application Server and are the principal names by which cells, nodes, servers, and clusters are known to z/OS.

Note: The z/OS operating system has an eight-character limit on many operating-system interface values.

Short names must be from one to eight characters long, can contain only uppercase alphabetic or numeric characters, and cannot begin with a numeric character.

You should limit your server short names to seven characters to allow the runtime to add an `S` or an `A` to a short name to designate servant regions or adjuncts. For example, a server short name of `BBOS001` results in `BBOS001S` for servant regions and `BBOS001A` for control region adjunct processes. If your standards require eight characters for server short names, explicitly set the short names of the servant and adjunct regions.

Wherever this article states that two names must be the same or different, this means that the long names must be the same or different and that the short names must also be the same or different. There is no requirement that the long and short names be related, but most users find it convenient to make them identical or at least similar to each other.

Choosing a cell name

The cell name identifies a WebSphere Application Server cell. Each of the following is a cell:

1. Standalone application server
2. Network Deployment cell, together with its nodes and servers
3. DMZ secure proxy server

4. Administrative agent
5. Job manager

Each cell must have cell name that it does not share with any other cell on the same system. If cells on different systems communicate with one another, they should not have the same cell name.

In order to federate a standalone application server into a Network Deployment cell, the standalone server's cell name must be different from the cell name of the Network Deployment cell.

Choosing a server name

The server name identifies a WebSphere Application Server server within the node to which it belongs. Each server must have server name that it does not share with any other server in the same node. On the z/OS operating system, the server short name is also used as the server's MVS job name; and therefore, no two servers with the same server short name can run on the same z/OS system at the same time even if they are in different cells.

Standalone application servers
A standalone application server usually has a single application server because the administrative console in a standalone application server cell can only control a single server. If the application server node is registered with an administrative agent, however, the administrative agent can be used to create additional servers.

Network Deployment cells
A Network Deployment cell has at least one server—the deployment manager in its own node—and some number of additional application servers, Web servers, proxy servers, and other types of servers.

Secure proxy servers, administrative agents, and job managers
Secure proxy servers, administrative agents, and job managers each have a single server.

Choosing cluster names and generic server short names

The cluster name identifies a WebSphere Application Server cluster—a collection of identical servers, potentially spanning several nodes or systems, that run the same applications. Both application servers and proxy servers can be clustered. Each cluster must have cluster name that it does not share with any other cluster in the same cell.

The cluster short name has a special function—it is used to identify the cluster servers to the z/OS Workload Management facility (WLM). Even nodes that have not been clustered have a server generic short name, also called a ″cluster transition name,″ that is used for the same purpose; when a cluster is created from an existing application server, the server's generic short name becomes the cluster name.

As a result, no two servers on the same z/OS system should have the same server generic short name unless they are in the same cluster. This rule applies to deployment managers, node agents, administrative agents, and job managers as well as to application servers and proxy servers.

Naming conventions

Because of the large number of names to be chosen, together with the requirements that some names be the same or be unique, it is helpful to have a standard method of choosing names that meets both the enterprise's business needs and the requirements of the WebSphere Application Server architecture.

WebSphere Application Server for z/OS provides two different naming conventions for cells, nodes, servers, and clusters.

Basic naming convention
This convention includes a set of fixed defaults that have been in place since WebSphere

Application Server for z/OS Version 4.0 with some adjustments to allow for new server types in Version 7.0. These defaults are intended for getting started with WebSphere Application Server on z/OS, and they only support a single server of each type on a given z/OS system. Additional servers require that the default values be changed.

Read “Basic naming convention” for more information on this naming convention.

Standard naming convention

This convention includes a set of structured defaults that use names generated from one- or two-character cell, cluster, and system identifiers that you choose during customization. These defaults are based on names recommended by the Washington Systems Center for use with their Configuration Spreadsheet; they support arbitrary numbers of cells, nodes, and servers; and they are intended for production environments.

Read “Standard naming convention” on page 75 for more information on this naming convention.

You can develop your own naming convention, but it should take into account the considerations discussed in this article and described in more detail in the related articles on the basic and standard naming conventions.

Basic naming convention

In WebSphere Application Server for z/OS, cells and nodes are created using customization jobs that are built using the Profile Management Tool or the zpmt command. When you use the Profile Management Tool to create these customization jobs, most fields are preset to default values. Fixed defaults are used that follow the basic naming convention if one- and two-character cell, cluster, and system identifier values are not specified during customization.

The basic naming convention is intended to assist you in gaining experience with WebSphere Application Server on z/OS, and it is suitable for small application environments consisting of a single application server or Network Deployment cell with one each of the other types of servers—administrative agent, job manager, and secure proxy server. If a Network Deployment cell is created, additional servers can be generated in the single application server node.

Default values for a standalone application server

By default, a standalone application server is build with cell short name `BBOBASE`, node short name `BBONODE`, and server short name `BBOS001`. The corresponding long names are cell name `bbobase`, node name `bbonode`, and server name `server1`. This illustrates the convention that the default long names are simply the lowercase forms of the corresponding short names, which only use uppercase letters, unless there is a traditional name such as `server1` or `proxy1` that is used instead. The server generic short name, which is used to identify the server to Workload Management, is `BBOC001`.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS70.BBOBASE.BBONODE.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv7config/bbobase/bbonode
```

This shows another feature of both the basic and standard naming conventions in WebSphere Application Server for z/OS Version 7.0. The cell and node short names are used to name the configuration file system and this file system’s mount point is based on the cell and node long names. This convention helps to familiarize installers with the relevant names in each cell and makes it easy to remount file systems in the appropriate places.

The following SAF groups and user IDs are created during customization:

WSCFG1	Configuration group Provides administration and server privileges
WSSR1	Servant group Provides privileges needed by servant regions
WSCLGP	Unauthenticated, local user, or guest group Provides basic privileges to access the cell but nothing more
WSCRU1	Controller user ID Controller, control region adjunct, and daemon started tasks
WSSRU1	Servant user ID Servant started tasks
WSADMIN	Administrator user ID Used for cell configuration and, in certain circumstances, as a WAS administrator
WSADMSH	Asynchronous administrator user ID Used to run administrative shell scripts under a started task
WSGUEST	Unauthenticated-user user ID (z/OS-managed security only) Represents an unknown user for security purposes

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOS001	BBO7ACR	Controller
BBOS001A	BBO7AAR	Control region adjunct (handles messaging tasks for the controller)
BBOS001S	BBO7ASR	Servant region
BBODMNB	BBO7DMNB	Location service daemon
--------	BBO7ADM	Asynchronous administrative cataloged procedure

Note that the cataloged-procedure names in the second column of this table provide the following:

- Product indication (`BBO`)
- Product version number (`7`)
- Indication of the type of server (`A` for application server)
- Two characters showing the started task type (`CR` for controller, `AR` for adjunct region, and `SR` for servant region)

This pattern is used throughout the basic naming convention. The daemon job name and cataloged-procedure names follow their own pattern.

Default values for a deployment manager

To build a Network Deployment cell, you start with a deployment manager. To allow a standalone application server that is also built with the defaults to be federated into the Network Deployment cell, you must choose a new cell name and node name for the deployment manager.

By default, a deployment manager is built with cell short name `BBOCELL`, node short name `BBODMGR`, and server short name `BBODMGR`. The corresponding long names are cell name `bbocell`, node name `bbodmgr`,

and server name dmgr. The deployment manager long name is fixed by the product architecture. The deployment manager can never be clustered; therefore, its default server generic short name, which is used to identify the deployment manager to Workload Management, is the same as the server short name: BBODMGR.

In versions of WebSphere Application Server for z/OS earlier than Version 7.0, the z/OS system name and sysplex name were used as cell names for the standalone application server and Network Deployment cell, respectively. This limited the old naming convention to a maximum of two cells for one z/OS system. In addition, there is no reason for a z/OS system name and its sysplex name to be different, causing a collision if the two values are used as names for different cells. In WebSphere Application Server for z/OS Version 7.0, fixed cell names are used to avoid these problems.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS70.BBOCELL.BBODMGR.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv7config/bbocell/bbodmgr
```

The SAF groups and user IDs created during customization have the same default names as for the standalone application server in order to make federation possible and minimize the number of security database entries that must be created. No asynchronous administrator user ID is created because a deployment manager does not need one.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBODMGR	BBO7DCR	Controller
BBODMGRS	BBO7DSR	Servant region
BBODMNC	BBO7DMNC	Location service daemon

The cataloged-procedure names follow the same pattern as for the standalone application server. The D in the controller and servant procedure names indicates a deployment manager, and the C at the end of the location service daemon job name and cataloged-procedure name indicate an ND cell (as opposed to the B used for a base or standalone application server cell). The B and C in these names are values inherited from previous releases.

Default values for a managed node

When a managed (custom) node—an application server node with no servers that is intended for federation into a Network Deployment cell—is built, the name of the cell into which it will be federated is not actually specified. The managed node is created with a temporary cell name that must be different from the Network Deployment cell name. Therefore, the same defaults are used as those used for a standalone application server. Although this means that the configuration file system and mount point incorporate the temporary cell name, this can be corrected manually during customization if necessary.

The SAF groups, user IDS, and cataloged-procedure names are the same as those used for a standalone application server. However, an empty managed node does not have an application server; it only has a node agent (for node administration) until new servers are created in the node. The node agent has default server short name BBON001 and server long name nodeagent, which is fixed by the product architecture.

Default values for an administrative agent

An administrative agent controls one or more standalone application servers without requiring that they be federated into a Network Deployment cell.

By default, an administrative agent is built with cell short name BBOADMA, node short name BBOADMA, and server short name BBOADMA. The corresponding long names are cell name bboadma, node name bboadma, and server name adminagent, which is fixed by the product architecture. Like a deployment manager, the administrative agent can never be clustered; therefore, its default server generic short name, which is used to identify the administrative agent to Workload Management, is also set to BBOADMA.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS70.BBOADMA.BBOADMA.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv7config/bboadma/bboadma
```

The SAF groups and user IDs created during customization have the same default names as those used for the standalone application server in order to make it possible to register the standalone application server with the administrative agent.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOADMA	BBO7GCR	Controller
BBOADMAS	BBO7GSR	Servant region
BBODMNG	BBO7DMNG	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use G to indicate an administrative agent.

This makes the MVS start command for the administrative agent very simple:

```
START
BBO7GCR,JOBNAME=BBOADMA,ENV=BBOADMA.BBOADMA.BBOADMA
```

Default values for a job manager

A job manager can control an administrative agent's registered application server nodes or a deployment manager and its managed and unmanaged nodes. In fact, it can manage several of each. On a system using the basic naming convention, you can register either the standalone application server (through its administrative agent) or a Network Deployment cell (through its deployment manager) with the job manager.

By default, a job manager is built with cell short name BBOJMGR, node short name BBOJMGR, and server short name BBOJMGR. The corresponding long names are cell name bbojmgr, node name bbojmgr, and server name jobmgr (which is fixed by the product architecture). Like a deployment manager, the administrative agent can never be clustered; therefore, its default server generic short name, which is used to identify the job manager to Workload Management, is also set to BBOJMGR.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS70.BBOJMGR.BBOJMGR.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv7config/bbojmgr/bbojmgr
```

The SAF groups and user IDs created during customization have the same default names used for the other server types.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOJMGR	BBO7JCR	Controller
BBOJMGRS	BBO7JSR	Servant region
BBODMNJ	BBO7DMNJ	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use `J` to indicate a job manager.

Default values for a secure proxy server

A secure proxy server is intended to run in the ″demilitarized″ zone (DMZ), across a firewall from the WebSphere Application Server cells for which it serves as a front end. Unlike a regular proxy server, it cannot be clustered; but it can be registered with an administrative agent to provide some remote administration capabilities.

By default, a secure proxy server is built with cell short name `BBOPROX`, node short name `BBOPROX`, and server short name `BBOPROX`. The corresponding long names are cell name `bboprox`, node name `bboprox`, and server name `proxy1`. The default server generic short name, which is used to identify the server to Workload Management, is `BBOPROX`.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS70.BBOPROX.BBOPROX.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv7config/bboprox/bboprox
```

The SAF groups and user IDs created during customization have the same default names used for the other server types.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOPROX	BBO7XCR	Controller
BBOPROXS	BBO7XSR	Servant region
BBODMNX	BBO7DMNX	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use `X` to indicate a secure proxy server.

Default values for a secure proxy administrative agent

A secure proxy server can be registered with an administrative agent to provide some remote administration capabilities.

By default, a secure proxy administrative agent is built with cell short name BBOPRXA, node short name BBOPRXA, and server short name BBOPRXA. The corresponding long names are cell name bboprxa, node name bboprxa, and server name adminagent. The default server generic short name, which is used to identify the administrative agent to Workload Management, is BBOPRXA.

The default dataset name for the configuration file system is the following:

```
OMVS.WAS70.BBOPRXA.BBOPRXA.HFS
(or .ZFS if a zFS file system is selected)
```

and it is mounted at the following location:

```
/wasv7config/bboprxa/bboprxa
```

The SAF groups and user IDs created during customization have the same default names used for the other server types.

The following job names and cataloged-procedure names are used for the various regions:

Job Name	Cataloged-Procedure Name	Region
BBOPRXA	BBO7YCR	Controller
BBOPRXAS	BBO7YSR	Servant region
BBODMNY	BBO7DMNY	Location service daemon

The job names and cataloged-procedure names are similar to those used for the deployment manager, but they use Y to indicate a secure proxy administrative agent.

As with the regular administrative agent, the MVS start command is very simple:

```
START
BBO7YCR,JOBNAME=BBOPRXA,ENV=BBOPRXA.BBOPRXA.BBOPRXA
```

Where to go next

The basic naming convention is adequate for an introduction to the WebSphere Application Server for z/OS product. However, most enterprises will want to create at least two application server nodes, whether for test and production or to allow for failover in a Network Deployment cell. For these configurations, you must use a more complex server naming convention.

The WebSphere Application Server for z/OS standard naming convention is a straightforward extension of the basic naming convention. The BBO and WS prefixes are replaced with a two-character cell identifier; this allows for several concurrent cells or groups of cells with similar administrative needs that sharing a common set of server user IDs. Cluster identifiers and a system identifier, which are specified during customization, provide additional flexibility. Read “Standard naming convention” on page 75 for more information.

Related concepts

“Application server naming conventions” on page 67
There are several names that you must specify during WebSphere Application Server for z/OS configuration. Although it is possible to assign names to WebSphere Application Server for z/OS objects on an ad-hoc basis, it is safer and more efficient to assign names in an orderly fashion.

“Standard naming convention”
In WebSphere Application Server for z/OS, cells and nodes are created using customization jobs that are built using the Profile Management Tool or the zpmt command. When you use the Profile Management Tool to create these customization jobs, most fields are preset to default values. Defaults are used that follow the standard naming convention if one- and two-character cell, cluster, and system identifier values are specified during customization.

Standard naming convention

In WebSphere Application Server for z/OS, cells and nodes are created using customization jobs that are built using the Profile Management Tool or the zpmt command. When you use the Profile Management Tool to create these customization jobs, most fields are preset to default values. Defaults are used that follow the standard naming convention if one- and two-character cell, cluster, and system identifier values are specified during customization.

The standard naming convention is suitable for both initial and production use, and it allows you to create groups of cells and servers with each group sharing a common set of user IDs and group names. A group of cells and servers is distinguished by sharing the same cell identifier.

How the standard naming convention differs from the basic naming convention

While the basic naming convention supports at most a single Network Deployment cell and a single application server node on a given z/OS system, the standard naming convention allows for the creation of up to 936 separate administrative groups, each corresponding to a single two-character cell identifier, on a single z/OS system. Each of these administrative groups can include the following:

- One Network Deployment cell
- Up to 36 application server nodes
- Administrative agents, job managers, and secure proxy servers

This administrative group is not actually a part of the WebSphere Application Server architecture; it simply represents the fact that on z/OS, a group of cells can use a common set of SAF groups and user IDs, which in turn simplifies the setup of connections between these cells. On the other hand, using different SAF groups and user IDs for separate cells provides for administrative and runtime separation so that the cells using different SAF identities can interact only in ways that you specify or not at all.

Selecting cell, system, and cluster identifiers

If you want to use the standard naming convention, specify a cell identifer, system identifier, and (in some cases) a cluster identifier when you configure a new WebSphere Application Server cell or node using the Profile Management Tool.

Cell identifier

This two-character, uppercase-alphanumeric value is used to construct the names of the SAF user IDs and groups that will be used for all cells and servers that share the same cell identifier. Together with the system identifier, it is used to build cell names, node names, and other values.

To simplify interaction between two cells, create them using the same cell identifier. To minimize or prevent interaction between two cells, create them using different cell identifiers.

Note:

- Separate Network Deployment cells must have separate cell identifiers.

- Up to 36 of each of the other types of WebSphere Application Server cells (standalone application servers, administrative agents, job managers, and secure proxies) can be created with the same cell identifier as long as a separate system identifier is chosen that distinguishes each cell from the others of the same type.
- If a standalone application server is to be federated into a Network Deployment cell, security setup is considerably simpler if the application server uses the same SAF user IDs and groups as the Network Deployment cell. If both are created using the standard naming convention, configure them using the same cell identifier.
- An administrative agent must run under the same SAF groups as the standalone application servers that it administers. Configure them with the same cell identifier.

System identifier

This one-character, uppercase-alphanumeric value is used to distinguish the application server nodes in a Network Deployment cell and the various types of other servers (standalone application servers, administrative agents, job managers, and secure proxy servers) from each other. The name comes from the practice of creating a Network Deployment cell with one application server node on each z/OS system that the cell spans. However, the one-character identifier can also be used to distinguish several nodes on the same z/OS system or to identify several single-node cells that have the same cell identifier. In these latter cases, the system identifier does not have to represent an actual z/OS system.

For a Network Deployment cell with one node per z/OS system, assign a single alphanumeric character to each z/OS system and use that value when configuring the federated or managed application server nodes on that system. For other types of cells, you can assign any desired convention for the system identifier as long as no two servers of the same type share both a cell identifier and a system identifier.

Cluster identifier

This two-character, uppercase-alphanumeric value is used to distinguish application servers within an application server node. In order to allow for any application server to be used as the basis of an application server cluster, create each unclustered application server in a Network Deployment cell with its own cluster identifer. In the examples at the end of this article, the cluster identifier is given as a two-digit number to make it easy to identify the parts of each name.

Default values for cell, node, and server names

One Network Deployment cell and up to 36 of each of the other cell types can be configured with the standard naming convention under a single cell identifier by assigning a unique system identifier to each of the other cell types. In other words, two standalone application servers or two job managers that share a common cell identifier must have separate system identifiers.

For cell identifier `aa` and system identifier `s`, the standard naming convention would assign the following cell and node names:

Name	ND Cell Deployment Manager	ND Cell Managed Node	Standalone Application Server	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Cell name	aaCELL	aaCELL	aaBASEs	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs
Node name	aaDMNODE	aaNODEs	aaNODEs	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs

Note that the Network Deployment cell has one deployment manager node and can have one application server node (managed or federated) for each system identifier. The node name for a standalone application server uses the same convention as the Network Deployment cell, allowing for easy federation. The other server types use the same value as the cell name and node name because none of them require multiple nodes or an elaborate naming convention.

All of the names used so far are uppercase because they are z/OS short names, such as the cell short name and node short name, which must be uppercase. Each of these values also has a mixed-case long name, which is the internal WebSphere Application Server version of the name. For convenience, the standard naming convention uses the same value for the long name as for the short name but changes it to lowercase.

Server names are constructed from the cell identifier, system identifier, and (in the case of application servers) the cluster identifier. A Network Deployment cell can have only one deployment manager, and each of the other non-application server types has only a single server. Each server is also assigned a generic short name that is used to identify the server to Workload Management and is also used as the initial cluster name for application servers being clustered.

For cell identifier `aa`, system identifier `s`, and cluster identifier `nn`, the standard naming convention would assign the following server names and generic server short names

Name	**ND Cell Deployment Manager**	**Application Server in an ND Cell or Standalone**	**Administrative Agent**	**Job Manager**	**Secure Proxy Server**	**Secure Proxy Administrative Agent**
Server name	aaDMGR	aaSRnns	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs
Generic name	aaDMGR	aaSRnns	aaADMAs	aaJMGRs	aaPROXs	aaPRXAs

This application server naming convention allows additional servers to be created in an application server node following the same naming convention, and it also makes clustering easier.

Defaults for SAF group and user ID names

For cell identifier `cc`, the following SAF groups and user IDs are created during customization:

ccCFG	Configuration group Provides administration and server privileges
ccSRVG	Servant group Provides privileges needed by servant regions
ccGUESTG	Unauthenticated, local user, or guest group Provides basic privileges to access the cell but nothing more
ccACRU	Controller user ID Controller, control region adjunct, and daemon started tasks
ccASRU	Servant user ID Servant started tasks
ccADMIN	Administrator user ID Used for cell configuration and, in certain circumstances, as a WAS administrator
ccADMSH	Asynchronous administrator user ID Used to run administrative shell scripts under a started task
ccGUEST	Unauthenticated-user user ID (z/OS-managed security only) Represents an unknown user for security purposes

Default values for configuration file system names and mount points

Each WebSphere Application Server cell or managed node has its own configuration file system, which might be either an HFS or zFS dataset. When cell, system, and cluster identifiers are specified during configuration, each configuration file system is assigned a unique dataset name:

OMVS.MNT.*cell_short_name*.*node_short_name*.HFS
(for an HFS data set)

OMVS.MNT.*cell_short_name*.*node_short_name*.ZFS
(for a zFS data set)

You can modify these names to fit local conventions, but make it clear which cell and node are associated with each dataset. The default mount points for these configuration file systems use the cell and node long names (simply lowercase versions of the long names by default) for readability:

/wasv7config/*cell_long_name*.*node_long_name*

The datasets can be renamed, but the mount points should not be changed after initial customization because they are referred to throughout the configuration files. One result of this is that when a standalone application server is federated into a Network Deployment cell, it retains its original configuration mount point even if that mount point contains the old (standalone) cell name. Users who know that a standalone application server is to be federated into a particular Network Deployment cell might want to manually update the configuration file system dataset name and mount point during creation of the standalone application server to reflect the node's eventual cell name.

Default values for job names and cataloged-procedure names

Most application servers consist of a controller (control region) and one or more servants (servant regions). An application server also has a messaging region called a ″control region adjunct.″ The job name for the control region is the same as the server short name. The initial job name for the servant consists of the server short name followed by an S, while the initial job name for the control region adjunct consists of the server short name followed by an A. (This is why server short names are customarily limited to a length of seven characters.)

Each control region, servant region, and control region adjunct requires a cataloged procedure that points to the server's configuration file system. In practice, this means that each node has its own controller, servant, and (in some cases) control region adjunct cataloged procedures; but the different servers in an application server node do not need their own cataloged procedures because they share a configuration file system.

For cell identifier aa and system identifier s, the standard naming convention would assign the following job names and cataloged-procedures names. In each case, the controller job or procedure name is given first and followed by the job or procedure name for the servant and (if present) the control region adjunct:

Name	ND Cell Deployment Manager	Application Server Node (Node Agent in ND Cell)	Application Nerver Node (Application Server)	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Controller job name	ccDMGR	ccAGNTs	ccSRnns	ccADMAs	ccJMGRs	ccPROXs	ccPRXAs
Servant job name	ccDMGRS	ccAGNTsS	ccSRnnsS	ccADMAsS	ccJMGRsS	ccPROXsS	ccPRXAsS
Adjunct job name			ccSRnnsA				
Controller procedure	ccDMGR	ccACRs	ccACRs	ccGCRs	ccJCRs	ccXCRs	ccYCRs

Name	ND Cell Deployment Manager	Application Server Node (Node Agent in ND Cell)	Application Nerver Node (Application Server)	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Servant procedure	ccDMGRS	ccASRs	ccASRs	ccGSRs	ccJSRs	ccXSRs	ccYSRs
Adjunct procedure			ccAARs				

Each WebSphere Application Server cell also requires a location service daemon, which is used for all nodes of the cell on a given z/OS system:

Name	ND Cell (All Nodes)	Standalone Application Server	Administrative Agent	Job Manager	Secure Proxy Server	Secure Proxy Administrative Agent
Daemon job name	ccDEMN	ccDEMNs	ccDMNGs	ccDMNJs	ccDMNXs	ccDMNYs
Daemon procedure	ccDEMN	ccDEMNs	ccDMNGs	ccDMNJs	ccDMNXs	ccDMNYs

Related concepts

“Application server naming conventions” on page 67
There are several names that you must specify during WebSphere Application Server for z/OS configuration. Although it is possible to assign names to WebSphere Application Server for z/OS objects on an ad-hoc basis, it is safer and more efficient to assign names in an orderly fashion.

“Basic naming convention” on page 69
In WebSphere Application Server for z/OS, cells and nodes are created using customization jobs that are built using the Profile Management Tool or the zpmt command. When you use the Profile Management Tool to create these customization jobs, most fields are preset to default values. Fixed defaults are used that follow the basic naming convention if one- and two-character cell, cluster, and system identifier values are not specified during customization.

Configuration Planning Spreadsheet for z/OS

The Configuration Planning Spreadsheet can be used to create a response file that can then be imported into the Profile Management Tool.

Before you begin

A well-constructed WebSphere Application Server for z/OS cell will have a set of names and ports that are consistent and orderly. To assist in that process, a Microsoft® Excel spreadsheet has been developed that takes as input a small set of key variables and produces a properly arranged set of names and ports and other values. The spreadsheet creates a response file format ready for copy-and-paste into a file, which may then be imported into the Profile Management Tool. The spreadsheet and Profile Management Tool combination greatly simplifies the process of creating a configuration and it enforces a number of naming best practices. The spreadsheet has proven to be an effective and time-saving tool for administrators of WebSphere Application Server for z/OS.

Refer to http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100999, for a white paper on the use of the Spreadsheet with the Profile Management Tool. This white paper is entitled Using zPMT and Spreadsheet to Build Quick Standalone and contains step-by-step examples that demonstrate how the spreadsheet and the Profile Management Tool can be used together. The spreadsheet itself can be downloaded from http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS1331.

Default port assignments

This article lists the default server values for WebSphere Application Server for z/OS.

WebSphere Application Server for z/OS port assignments

Table 3. Default port assignments for WebSphere Application Server for z/OS

Port Name	Default Value					
	Standalone Application Server	Deployment Manager	ND Node Agent	ND Managed Node	Administrative Agent	Job Manager
HTTP Transport Port (WC_defaulthost)	9080			9080		
HTTPS Transport Secure Port (WC_defaulthost_secure)	9443			9443		
Administrative Console Port (WC_adminhost)		9060		9060	9060	9960
Administrative Console Secure Port (WC_adminhost_secure)		9043		9043	9043	9943
Administrative Interprocess Communication Connector Port (IPC_CONNECTOR_ADDRESS)	9633	9632			9630	9631
Bootstrap Port (BOOTSTRAP_ADDRESS)	2809	9809	2809	9810		
ORB	2809	9809	2809	9810	9807	9808
ORB SSL	0	0	0	0	0	0
SOAP/JMX (SOAP_CONNECTOR_ADDRESS)	8880	8879	9360	8880	8877	8876
Node Discovery Address (NODE_DISCOVERY_ADDRESS)			7272			
Node Multicast Discovery Address (NODE_MULTICAST_DISCOVERY_ADDRESS)			5000			
Cell Discovery Address (CELL_DISCOVERY_ADDRESS)		7277				
Service Integration Port (SIB_ENDPOINT_ADDRESS)	7276					
Service Integration Secure Port (SIB_ENDPOINT_SECURE_ADDRESS)	7286					
Service Integration MQ Interoperability Port (SIB_MQ_ENDPOINT_ADDRESS)	5558					

Table 3. Default port assignments for WebSphere Application Server for z/OS (continued)

Port Name	Default Value					
	Standalone Application Server	**Deployment Manager**	**ND Node Agent**	**ND Managed Node**	**Administrative Agent**	**Job Manager**
Service Integration MQ Interoperability Secure Port (SIB_MQ_ENDPOINT_SECURE_ADDRESS)	5578					
Session Initiation Protocol Port (SIP_DEFAULTHOST)	5060					
Session Initiation Protocol Secure Port (SIP_DEFAULTHOST_SECURE)	5061					
High Availability Manager Communications (DCS_UNICAST_ADDRESS)	9353	9352	9354			
DataPower® Application Manager		5555				
Daemon Port	5655	5755				
Daemon SSL Port	5656	5756				

Location service daemon ports

Standalone application server node location service daemons are considered temporary. The ports assigned to a standalone application server node's location service daemon are used only until that node is federated. It is advisable to set aside a couple of ports to serve as ″interim ports″ for the standalone application server node location service daemon. The ″permanent″ location service daemon ports are the ones assigned to the deployment manager. Those same ports are copied to location service daemons created when a standalone application server node on another MVS image is federated into the deployment manager cell.

Node agent ports

There is a node agent per MVS image on which the cell spans. One design option calls for all node agents to have the exact same ports so the Sysplex Distributor is able to balance the traffic between the two. The node agent is created when the BBOWADDN customized job is run.

Server clusters

A server cluster is a grouping of two or more servers into a one logical server. A cluster is created through the administrative console. Servers within a cluster are called ″cluster members.″ Servers (″members″) within a cluster start out being clones of one another. When it comes to the TCP ports for the members in a cluster, the administrative console allows you during the creation of the cluster to specify if you want the HTTP ports to be unique or the same. The other ports -- bootstrap, DRS, ORB, ORB SSL and SOAP -- will be made unique by the application server.

For complex configurations with multiple members in a cluster it is advisable to make the members be as nearly identical to one another as possible, including the TCP ports. Therefore, when planning it is recommended a range of ports be allocated for a cluster with the intention to make certain all members of that cluster were given the same set of ports. Because WebSphere will automatically generate unique

DRS, ORB, ORB SSL and SOAP ports for the second cluster member, it is necessary to go back in and remap the ports back to the ports set aside for the server cluster

Note: When a ″vertical cluster″, two members on the same MVS image, is the potential configuration, you will need to consider port sharing by two members of the same cluster on the same MVS image.

Initial security configuration

During installation you now have the option of enabling administrative security during initial cell customization, this procedure is referred to as ″security out of the box″. This protects the cell from unauthorized modification, which can occur if security is not enabled.

When a new standalone application server or Network Deployment cell is created, there are three initial security choices in WebSphere Application Server for z/OS Version 7.0:

- Use a z/OS security product to manage user identities and authorization policy
- Use WebSphere Application Server to manage user identities and the authorization policy
- Do not enable security

This article describes the three initial security options and the configuration effects of each.

Remember that WebSphere Application Server for z/OS always requires the presence of a SAF-compliant security system to provide operating system security. Regardless of which security option is chosen:

- SAF user IDs for WebSphere Application Server started tasks are always created during customization.
- SAF groups are created for the configuration, servant and local user groups are created during customization, and granted necessary permissions
- SAF SERVER profiles are used to control servant access to controller regions.
- If daemon SSL is selected during customization, a key ring and digital certificate for the daemon are created in SAF.

Note: Each of the initial security configurations is basic, requiring few choices during customization; after configuration is complete, additional work is usually required to match cell security policies to the needs of the enterprise. See the Security section of the InfoCenter for more information.

Option 1: Use a z/OS security product to manage user identities and authorization policy

If this option is chosen during customization:

1. Each WebSphere Application Server user and group identity corresponds to a user ID or group in the z/OS system's SAF-compliant security system (IBM'S RACF, or an equivalent product).
2. Access to WebSphere Application Server roles is controlled using the SAF EJBROLE profile.
3. Digital certificates for SSL communication are stored in the z/OS security product.

The z/OS system's security product is always used to control WebSphere Application Server for z/OS started task identities, and the location service daemon's digital certificate (if daemon SSL is selected). However, when this security option is selected, all WebSphere Application Server administrators and administrative groups must be defined to SAF as well. Later, if application security is enabled, the SAF security database holds those user identities as well.

This option is appropriate when servers or cells will reside entirely on z/OS systems, with SAF as the user registry. Customers who plan to implement an LDAP or custom user registry, but who will map WebSphere Application Server identities to SAF identities and use EJBROLE profiles for authorization, should also choose this option so that initial SAF EJBROLE setup is performed.

When this option is chosen during customization, the following SAF user IDs are created:

- An administrator user ID
- An ″unauthorized user″ ID, to represent WebSphere Application Server identities which have not been authenticated

SAF EJBROLE profiles for administrative roles (administrator, configuration, deployer, monitor and operator) are created, and the administrator user ID is granted the administrator role.

SAF CBIND profiles are created, and granted to the configuration group.

Digital certificates are created in the SAF security system for each server controller (deployment manager or application server controller).

Digital key rings are created in the SAF security system for the administrator, controller, controller region adjunct, and server user IDs, and the appropriate certificates are attached to these key rings.

A SAF profile prefix may be specified when this option is chosen; the SAF profile prefix becomes part of the APPL, CBIND and EJBROLE profile names used for authorization checking.

Option 2: Use WebSphere Application Server to manage user identities and authorization policy

If this option is chosen during customization:

1. Each WebSphere Application Server user and group identity corresponds to an entry in a WebSphere Application Server user registry. The initial user registry is a simply file-based user registry, created during customization, and residing in the configuration file system.
2. Access to WebSphere Application Server roles is controlled using WebSphere Application Server role bindings. In particular, administrative roles are controlled using the ″Console users and groups″ settings in the administrative console.
3. Digital certificates for SSL communication are stored in the configuration file system.

The z/OS system's security product is always used to control WebSphere Application Server for z/OS started task identities, and the location service daemon's digital certificate (if daemon SSL is selected). However, when this security option is selected, all WebSphere Application Server users and groups for administrative access are defined in the WebSphere user registry, rather than in SAF. Later, if application security is enabled, the WebSphere Application Server user registry holds those user identities as well.

This option is appropriate when servers or cells will reside on a mix of z/OS and non-z/OS systems, as well as for customers who plan to implement an LDAP or custom user registry to replace the initial registry. (Customers who plan to implement an LDAP or custom user registry with identity mapping to SAF should select z/OS-managed security during customization; see above.)

When this option is chosen during customization, a file-based user registry is created in the configuration file system.

An administrator user ID (and an optional samples user ID and group) are added to the file-based user registry.

The administrator user ID is added to the list of authorized console users.

Self-signed digital certificates for servers are created in the configuration file system automatically by WebSphere Application Server.

Option 3: Do not enable security

If this option is chosen, no administrative security is configured. Anyone with access to the administrative console port can make changes to the server or cell configuration.

A post-customization security setup is recommended.

The initial security setup options in WebSphere Application Server are very basic, and are intended only to provide initial administrative security. After your server or cell is up and running, you may wish to:

- Switch to another user registry. You can use LDAP or a custom user registry instead of the SAF security database or file-based registry.
- Define additional administrators, or distribute administrative roles
- Implement application security

Building a practice WebSphere Application Server for z/OS cell

Use this task to practice configuring WebSphere Application Server for z/OS. If you are installing the product for the first time without migration from an earlier version, it is helpful to install a practice application serving environment in order to learn the customization process.

Before you begin

Note the following when you install your practice runtime:

- Be careful when typing and following the instructions in the customization.
- Note the user ID requirements in the generated instructions. If your user IDs are not configured correctly, the jobs might not run successfully.
- Keep track of each step so that you do not skip or repeat any steps.
- Examine each job's output (not only the return code) to confirm that everything is configured correctly. Sometimes, the return code indicates no problems but the job output contains errors. For a proper configuration, you should have no errors in your job output unless the instructions specifically describe errors in the job output.

About this task

You should install a practice runtime when you install WebSphere Application Server on z/OS for the first time and want to learn the steps for installing and customizing it.

Install using either the Profile Management Tool or the zpmt command.

1. Print a copy of the "Customization worksheet: Standalone application server for Version 7.0" on page 101 and fill it out using "Customization variables: Standalone application server cell" on page 86 as a guide.

   Note: Make sure that the user ID names, group names, UID/GID values, and TCP/IP port numbers that you specify are not already being used on your z/OS system.
2. Read the topic in "Using the Profile Management Tool" on page 287.
3. Follow the steps in "Creating a standalone application server cell" on page 291. View and follow the generated instructions, which tell you how to:
   - Perform the manual configuration updates in the generated standalone application server instructions. These steps affect parts of your system that are usually controlled. These are changes that the systems programmer responsible for your z/OS system should review.
   - Update your server-specific security definitions.

     The next job (BBOCBRAK) issues the RACF commands necessary for defining the users, groups, profiles, and permissions for the WebSphere Application Server for z/OS runtime servers. Submit

the BBOCBRAK job, or take it to your security administrator for approval. Your security administrator should issue those commands or submit the supplied jobstreams. If your installation has a different profile structure, you might have to modify the RACF commands generated by this exec to suit your particular needs.

Note: Your installation must have ″list of groups″ on for these commands to work because the servers must be connected to the WebSphere Application Server for z/OS administrator group.

- Create the configuration file system and WebSphere Application Server for z/OS home directory for your server. Jobs BBOWCFS and BBOWHFSA (run at this point) and job BBOWWPFA (see below) run BPXBATCH shell scripts to define, customize, and load data into the configuration HFS and manipulate the ownership and permission attributes. For this reason, you must run these jobs under a user ID with UID=0.
- Create cataloged procedures for the server.
- Set up the runtime (configuration) file system for the new application server. The BBOWWPFA job might run for some time. The BBOWHFSB job cleans up the configuration file system and makes sure that all file ownerships are correct.
- Start the new standalone application server, and run the Install Verification Test (IVT).

Note:

- If the BBOWWPFA (profile creation) job fails with the following error:

  ```
  Cannot use the directory: The /WebSphere/V7R0M0/AppServer/profiles/default directory exists and is not empt
  INSTCONFFAILED: Cannot create profile: The profile does not exist.
  ```

  delete the *was_home*/profiles/default directory and all its contents before rerunning BBOWWPFA.
- If you have some other security product such as Top Secret or ACF2 instead of RACF, contact your security system vendor for the appropriate security system commands needed to configure WebSphere Application Server for z/OS. You might need to contact the vendor for the latest maintenance and guidance on WebSphere Application Server for z/OS customization.

4. Troubleshoot any problems you encounter while customizing your application server.

   If you encounter problems while customizing your application server, review the steps that you have performed--especially regarding such things as specific user IDs under which jobs must be run. Check all job output for any error messages that you might have missed. See Chapter 11, “Troubleshooting installation and configuration,” on page 391 for additional advice.

   Watch out for these common mistakes:

   - Navigating the configuration file system with a UID of ″0″ can alter files or their ownership and permission attributes, making them inaccessible to the WebSphere Application Server for z/OS runtime servers and administrators. To avoid this problem, use the WebSphere Application Server for z/OS administrator user ID.
   - If you decide to change any of the customized variables after you submit any of these jobs, do not make manual modifications to the generated jobstreams or data. Cancel the installation, and start over by regenerating all the jobstreams and start over from the BBOWHFSA job.

Results

After you have successfully followed the instructions, you will have set up a WebSphere Application Server for z/OS standalone application server.

What to do next

Read the concept articles under Chapter 8, “Planning for product configuration,” on page 49 and plan one or more application serving environments that fit your system environment and business needs.

You might want to delete the practice application server that you just set up in order to save space on your system, to clean up your datasets, or for other reasons. Follow these steps to delete it from your system:

1. Stop the server.
2. Unmount and delete the configuration file system.
3. Delete the cataloged procedures.
4. Remove any TCP/IP port reservations for the practice application server.
5. Delete the RACF user IDs, groups, and profiles that you have created unless you use the same users and groups for a different WebSphere Application Server for z/OS cell.

Planning for a standalone application server cell

About this task

A standalone application server cell is the simplest WebSphere Application Server for z/OS configuration on which you can deploy and run applications. A standalone application server cell includes the following:

- A basic cell and node configuration
- A location service daemon
- An application server that runs the administrative console application. You can deploy and run additional applications on this server.

You cannot add additional servants to an application server running the standalone version of the administrative console application. You can define additional application servers in the standalone cell, but you cannot control them using the administrative console. For more complicated or robust WebSphere Application Server for z/OS application-serving environments, the Network Deployment cell configuration is recommended.

If you have never configured a WebSphere Application Server for z/OS cell, try “Building a practice WebSphere Application Server for z/OS cell” on page 84 first.

1. Print a copy of “Customization worksheet: Standalone application server for Version 7.0” on page 101.
2. Fill out the worksheet as described in “Customization variables: Standalone application server cell.”
3. Save the worksheet for use during standalone application server customization.

Customization variables: Standalone application server cell

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a standalone application server cell.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name
Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)
Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

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

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

Name and userid defaults
Set default names and user IDs based on cell, cluster, and system identifiers

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

Application server will be federated into a Network Deployment cell
Select this option to indicate that the application server will be federated into a Network Deployment cell. In this case, specify the two-character cell identifier of the target Network Deployment cell.

Two-character cell identifier
Two-character cell identifier to be used to create default names and user IDs

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

Two-character cluster identifier
Two-character cluster identifier to be used to create default names and user IDs

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

Single-character system identifier
Single-character system identifier to be used to create default names and user IDs

Note: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults
Select default port values from the following port range

When this option is not selected, each port value defaults to an IBM-provided number. When this option is selected, each port default value is selected from the following port number range.

The port range must contain at least 20 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the servant group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs (provides minimal access to the cell)

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID
User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
User identifier associated with the control region user ID

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

Common servant user ID

User ID
User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID
User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the administrator user ID

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

Asynchronous administration user ID
User ID used to run asynchronous administration operations procedure

It must be a member of the WebSphere Application Server configuration group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
UNIX System Services UID number for the asynchronous administration task user ID.

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

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name
Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

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

Note:

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

Long name
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.

Note:

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

Node names

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

Note:

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

Long name
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.

Note:

- Name must be 50 or fewer characters.
- 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.

Server names

Short name
Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server job name.

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

Long name
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.

Note:

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

Cluster transition name
WLM APPLENV (WLM application environment) name for this server

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. See “Cataloged procedures” on page 54 for more information.

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

JVM mode

31 bit Specifies that the JVM in each application server is to run in 31-bit mode

64 bit Specifies that the JVM in each application server is to run in 64-bit mode

Configuration File System

Note: The cell long name is included in the default mount point and the cell short name is included in the default dataset name. You might want to change the cell long and short names in these default values to the actual long and short names of the cell into which this node will be federated.

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

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

This is the SMP/E installation directory.

Read "Product file system" on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Optional Application Deployment

Deploy the administrative console
Specify whether to install a Web-based administrative console that manages the application server.

Deploying the administrative console is recommended, but if you deselect this option, the information center contains detailed steps for deploying it after the profile exists.

Deploy the default application
Specify whether to install the default application that contains the Snoop, Hello, and HitCount servlets.

Deploy the sample applications
Specify whether to install the sample applications (the Samples Gallery).

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.

Process Definitions

Controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Controller adjunct process

Job name
Job name used by WLM to start the control region adjunct

This is set to the server short name followed by the letter ″A″, and it cannot be changed through the tool.

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

Note: Name must be seven or fewer characters.

Servant process

Job name
Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter ″S″, and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Admin asynch operations procedure name
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

Read “Cataloged procedures” on page 54 for more information.

Port Values Assignment

Node host name or IP address
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.

JMX SOAP connector port
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.

Note: Value cannot be 0.

ORB listener IP address
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
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

HTTP transport IP address
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. 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
Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port
Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

HTTP transport port
Port for HTTP requests (WC_defaulthost)

Note: Value cannot be 0.

HTTPS transport port
Port for secure HTTP requests (WC_defaulthost_secure)

Note: Value cannot be 0.

Administrative interprocess communication port (K)
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 (DCS)
Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Note: Value cannot be 0.

Service integration port
Port for service-integration requests (SIB_ENDPOINT_ADDRESS)

Note: Value cannot be 0.

Service integration secure port
Port for secure service-integration requests (SIB_ENDPOINT_SECURE_ADDRESS)

Note: Value cannot be 0.

Service integration MQ interoperability port
Port for service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_ADDRESS)

Note: Value cannot be 0.

Service integration MQ interoperability secure port
Port for secure service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_SECURE_ADDRESS)

Note: Value cannot be 0.

Session initiation protocol (SIP) port
Port for session initiation requests (SIP_DEFAULTHOST)

Note: Value cannot be 0.

Session initiation protocol (SIP) secure port
Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Note: Value cannot be 0.

Location Service Daemon Definitions

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 enterprise beans for example) establish connections to the location service daemon first, then forward them to the target application server.

Daemon home directory
Directory in which the location service daemon resides

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

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

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

Note: Name must be seven or fewer characters.

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

The default value 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.

Listen IP
Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

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

Register daemon with WLM DNS
If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it; otherwise, do not select it.

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

Note: If you plan to federate this application server into a Network Deployment cell, you might want to set the application server's SAF key ring name to be the same as that of the Network Deployment cell.

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

Generate certificate authority (CA) certificate
Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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
Select this option if you want to enable writable SAF key ring support

Enable SSL on location service daemon
Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product
Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server
Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

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

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security
Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Security Managed by the z/OS Product

Note: If you plan to federate this application server into a Network Deployment cell, you might want to set the application server's SAF profile prefix to be the same as that of the Network Deployment cell.

SAF profile prefix (optional)
SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID
User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the ″guest″ user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name
User name for the administrator

Password
Password for the administrator

Note: This password must not be blank.

Specify a user name and password to login to the Samples user account.

Sample applications

User name
User name for the samples user account

Password
Password for the samples user account

Security Certificate

Default personal certificate

Issued to distinguished name
Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name
Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

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

Root signing certificate

Expiration period in years
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
Default password for all keystores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Web Server Definition

Note:

- You will not be able to administer a Web server through the integrated solutions console on a standalone application server until it is federated.
- You can only have one Web server defined on a standalone application server.

Create a Web server definition
Indicates whether to create a Web server definition.

You can only have one Web server defined on a standalone application server.

Web server type
Select the Web server type from the list of supported Web servers.

Web server operating system
Operating system where the Web server is located

Web server name
Name used in defining the Web server to WebSphere Application Server

Web server host name or IP address
IP name or address of the system on which the Web server is located

Web server port
HTTP port on which the Web server listens

Web server installation directory path
Name of the directory where the Web server is installed

Web server plug-in installation directory path
Name of the directory in where the Web server plug-ins are installed

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Standalone application server for Version 7.0

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: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZAppSrv*xx*	
Response file path name (optional)	None	

Default 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			

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

Target Datasets

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

Configure Common Groups

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

Configure Common Users

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

System and Dataset Names

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

Cell, Node, and Server Names

Item		Default	Your value
Cell names			
	Short name	BBOBASE	
	Long name	bbobase	
Node names			
	Short name	BBONODE	
	Long name	bbonode	
Server names			

Item		Default	Your value
	Short name	BBOS001	
	Long name	server1	
Cluster transition name		BBOC001	
JVM mode			
	31 bit	Not selected	
	64 bit	Selected	

Configuration File System

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	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.			

WebSphere Application Server Product File System

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	

Optional Application Deployment

Item	Default	Your value
Deploy the administrative console	Selected	

Item	Default	Your value
Deploy the default application	Selected	
Deploy the sample applications	Not selected	

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7ACR	
Controller adjunct process			
	Job name	*server_short_name*A	*server_short_name*A
	Procedure name	BBO7CRA	
Servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO7ASR	
Admin asynch operations procedure name		BBO7ADM	

Port Values Assignment

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	
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	

Item	Default	Your value
Session initiation protocol (SIP) port	5060	
Session initiation protocol (SIP) secure port	5061	

Location Service Daemon Definitions

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	

SSL Customization

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 writable SAF keyring support	Not selected	
Enable SSL on location service daemon	Selected	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item	Default	Your value
SAF profile prefix	*cell_short_name*	
WebSphere Application Server unauthenticated user		

Item			Default	Your value
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

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

Security Certificate

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

Web Server Definition (Part 1)

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	*host_name*	
	Web server port	80	

Web Server Definition (Part 2)

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

Job Statement Definition

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

Customization worksheet: Standalone application server for Version 6.1

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: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZAppSrv*xx*	
Response file path name (optional)	None	

Default 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			

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

Target Datasets

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

Configure Common Groups

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

Configure Common Users

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

Names and Dataset Qualifier

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	
Websphere product dataset high-level qualifier	None	

Product Datasets

Item	Default	Your value
SBBOLPA dataset name or catalog alias	*product_hlq*.SBBOLPA	
SBBOEXEC dataset name	*product_hlq*.SBBOEXEC	
SBBOMSG dataset name	*product_hlq*.SBBOMSG	
SBBOLOAD dataset name or catalog alias	*product_hlq*.SBBOLOAD	

Item	Default	Your value
SBBGLOAD dataset name or catalog alias	*product_hlq*.SBBGLOAD	
SBBOLD2 dataset name or catalog alias	*product_hlq*.SBBOLD2	
Run WebSphere Application Server from STEPLIB	Selected	

Cell, Node, and Server Names

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	

Configuration File System

Item		Default	Your value
Mount point		/wasv61config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point		AppServer	
Dataset name		OMVS.WAS61.*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	

WebSphere Application Server Product File System

Item	Default	Your value
Product file system directory	/usr/lpp/zWebSphere/V6R1	

Item			Default	Your value
Intermediate symbolic link				
	Create intermediate symbolic link		Selected	
		Path name of intermediate symbolic link	/wasv61config/ *cell_long_name*/ *node_long_name*/ wassmpe	

Optional Application Deployment

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

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO6ACR	
Controller adjunct process			
	Job name	*server_short_name*A	*server_short_name*A
	Procedure name	BBO6CRA	
Servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO6ASR	
Admin asynch operations procedure name		BBOW6SH	

Port Values Assignment

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		*	

Item		Default	Your value
	Administrative console port	9060	
	Administrative console secure port	9043	
	HTTP transport port	9080	
	HTTPS transport port	9443	
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	

Location Service Daemon Definitions

Item	Default	Your value
Daemon home directory	/wasv61config/ *cell_long_name*/ *node_long_name*/Daemon	/wasv61config/*cell_long_name*/ *node_long_name*/ Daemon
Daemon job name	BBODMNB	
Procedure name	BBO6DMN	
IP name	*host_name*	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

SSL Customization

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	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			*cell_short_name*	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

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

Web Server Definition (Part 1)

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	*host_name*	
	Web server port	80	

Web Server Definition (Part 2)

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

Job Statement Definition

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

Planning for an administrative agent

An administrative agent provides a single interface to administer multiple standalone application servers in environments such as development and unit test.

About this task

An administrative agent can monitor and control multiple application servers on one or more nodes. By using a single interface to administer your application servers, you reduce the overhead of running administrative services in every application server.

Use the following commands to register and unregister a node with the administrative agent:

- registerNode

  Run the registerNode command to register a node with the administrative agent. When you run the command, the standalone node is converted into a node that the administrative agent manages. The administrative agent and the node being registered must be on the same system. You can only run the command on an unfederated node. If the command is run on a federated node, the command exits with an error.

  Any node registered with the administrative agent automatically becomes eligible to register with the job manager.
- deregisterNode

  Use the deregisterNode command to deregister a node from an administrative agent so that you can use the node standalone or register the node with another administrative agent. The node must have been previously registered with the administrative agent. When you deregister a node, the node configuration is retained but is marked as not registered with the administrative agent.

An administrative agent can register any of the profiles that it manages with a job manager.

For more information, read the ″Administering nodes using the administrative agent″ article in the information center.

1. Print a copy of “Customization worksheet: Administrative agent” on page 127.
2. Fill out the worksheet as described in “Customization variables: Administrative agent.”
3. Save the worksheet for use during administrative agent customization.

Customization variables: Administrative agent

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure an administrative agent.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name
Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)
Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Server Type Selection

Server type
Type of server to be created within this management profile

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

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

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

Name and userid defaults
Set default names and user IDs based on cell and system identifiers

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

Two-character cell identifier
Two-character cell identifier to be used to create default names and user IDs

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

Single-character system identifier
Single-character system identifier to be used to create default names and user IDs

Note: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults
Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the servant group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID
User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
User identifier associated with the control region user ID

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

Common servant user ID

User ID
User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID
User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the administrator user ID

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

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

System name

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

Sysplex name

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name

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

Cell, Node, and Server Names

Cell names

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

Short name

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

Note:

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

Long name

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

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

Note:

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

Node names

Short name

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

Note:

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

Long name

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

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

Note:

- Name must be 50 or fewer characters.

- Name must be unique within the cell.

Server names

Short name
Name that identifies the server to z/OS facilities such as SAF

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

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

Long name
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.

Note: Name must be 50 or fewer characters.

Cluster transition name
WLM APPLENV (WLM application environment) name for this server

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. See “Cataloged procedures” on page 54 for more information.

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

Configuration File System

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

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

This is the SMP/E installation directory.

Read “Product file system” on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Process Definitions

Controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Servant process

Job name
Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter ″S″, and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address
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.

JMX SOAP connector port
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.

Note: Value cannot be 0.

ORB listener IP address
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
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

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

HTTP transport IP address
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. 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
Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port
Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

Administrative interprocess communication port (K)
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).

Location Service Daemon Definitions

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
Directory in which the location service daemon resides

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

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

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

Note: Name must be seven or fewer characters.

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

The default value 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.

Listen IP
Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

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

Register daemon with WLM DNS
If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

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

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

Generate certificate authority (CA) certificate
Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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
Select this option if you want to enable writable SAF key ring support

Enable SSL on location service daemon
Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product
Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server
Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

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

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security
Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Security Managed by the z/OS Product

SAF profile prefix (optional)
SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID
User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the ″guest″ user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name
User name for the administrator

Password
Password for the administrator

Note: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name
Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name
Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

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

Root signing certificate

Expiration period in years
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
Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Administrative agent

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 administrative agent:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZManagement*xx*	
Response file path name (optional)	None	

Server Type Selection

Item	Default	Your value
Server type	Deployment manager	Administrative agent

Default 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	9510	
		Highest default port number	9519	

Target Datasets

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

Configure Common Groups

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

Item				Default	Your value
	Group			WSCLGP	
		Allow OS security to assign GID		Not selected	
		Allow user-specified GID		Selected	
			Specified GID	2502	

Configure Common Users

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

System and Dataset Names

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

Cell, Node, and Server Names

Item		Default	Your value
Cell names			
	Short name	BBOADMA	
	Long name	bboadma	
Node names			
	Short name	BBOADMA	
	Long name	bboadma	

Item		Default	Your value
Server names			
	Short name	BBOADMA	
	Long name	adminagent	adminagent
Cluster transition name		BBOADMA	

Configuration File System

Item		Default	Your value
Mount point		/wasv7config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point		AdminAgent	
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	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.			

WebSphere Application Server Product File System

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	

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7GCR	
Servant process			

Item		Default	Your value
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO7GSR	

Port Values Assignment

Item		Default	Your value
Node host name or IP address		None	
	JMX SOAP connector port	8877	
ORB listener IP address		*	
	ORB port	9807	
	ORB SSL port	0	
HTTP transport IP address		*	
	Administrative console port	9060	
	Administrative console secure port	9043	
Administrative interprocess communication port (K)		9630	

Location Service Daemon Definitions

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	BBODMNG	
Procedure name	BBO7DMNG	
IP name	*host_name*	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

SSL Customization

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*	

Item	Default	Your value
Enable writable SAF keyring support	Not selected	
Enable SSL on location service daemon	Selected	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			*cell_short_name*	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

Item	Default	Your value
User name	WSADMIN	
Password	None	

Security Certificate

Item		Default	Your value
Default personal certificate			
	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			

Job Statement Definition

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

Planning for a Network Deployment cell

This article covers the requirements for a Network Deployment cell.

About this task

A Network Deployment cell is a full-function WebSphere Application Server for z/OS configuration on which you can deploy and run applications. A Network Deployment cell includes the following:

- A cell configuration.
- A deployment manager that runs the administrative console application.
- One or more application server nodes (one is recommended) on each z/OS target system hosting portions of the cell. Each node consists of a node agent and some number of application servers.
- A single location service daemon on each z/OS system.

This part of the configuration process creates the initial cell configuration, the deployment manager, and a location service daemon for the z/OS system on which the deployment manager runs. Once the Network Deployment cell is created, add application server nodes by creating and federating new managed nodes, or by federating standalone application server nodes into the Network Deployment cell.

When configuring your deployment manager node, keep the following in mind:

- When allocating target datasets for this option, it is possible, though not recommended, to use the same target datasets that you used for the standalone application server node. The job names for each configuration are very close to one another; and if you use the same target datasets, you might find it difficult to keep the two sets of jobs separate. Therefore, it is better to create a new set of target datasets and keep the two sets of jobs separate from one another.
- If possible, set up your file system such that the root file system is shared among all processors and the deployment manager's configuration is in a configuration HFS on a system-generic mount point.

  Note: This configuration scenario is the best for certain tasks, such as starting the deployment manager on another system, that you might want to perform in the future.

1. Print a copy of "Customization worksheet: Deployment manager for Version 7.0" on page 145.
2. Fill out the worksheet as described in "Customization variables: Deployment manager."
3. Save the worksheet for use during Network Deployment cell customization.

Customization variables: Deployment manager

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a deployment manager.

The WebSphere Application Server for z/OS runtime requires four servers in a Network Deployment cell: application server, deployment manager, node agent, and location service daemon. The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for a deployment manager.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name
Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)
Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Server Type Selection

Server type
Type of server to be created within this management profile

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

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

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

Name and userid defaults
Set default names and user IDs based on a cell identifier

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

Two-character cell identifier
Two-character cell identifier to be used to create default names and user IDs

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

Port defaults
Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 20 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the servant group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID
User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
User identifier associated with the control region user ID

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

Common servant user ID

User ID
User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID
User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the administrator user ID

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

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name
Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

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

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

Note:

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

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

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

Note:

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

Node names

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

Note:

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

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

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

Note:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names

Short name
Name that identifies the server to z/OS facilities such as SAF

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

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

Long name
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.

Note: Name must be 50 or fewer characters.

Cluster transition name
WLM APPLENV (WLM application environment) name for this server

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. See “Cataloged procedures” on page 54 for more information.

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

Configuration File System

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

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

This is the SMP/E installation directory.

Read “Product file system” on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Process Definitions

Controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Servant process

Job name
Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter ″S″, and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address
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.

JMX SOAP connector port
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.

Note: Value cannot be 0.

Cell discovery address port
Port number used by node agents to connect to this deployment manager server (CELL_DISCOVERY_ADDRESS)

ORB listener IP address
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
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

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

HTTP transport IP address
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. 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
Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port
Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

Administrative interprocess communication port (K)
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 (DCS)
Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Note: Value cannot be 0.

DataPower appliance manager secure inbound port
Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager (DataPowerMgr_inbound_secure)

Location Service Daemon Definitions

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
Directory in which the location service daemon resides

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

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

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

Note: Name must be seven or fewer characters.

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

The default value 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.

Listen IP
Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

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

Register daemon with WLM DNS
If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

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

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

Generate certificate authority (CA) certificate
Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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
Select this option if you want to enable writable SAF key ring support

Enable SSL on location service daemon
Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product
Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server
Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

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

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security
Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Security Managed by the z/OS Product

SAF profile prefix (optional)
SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID
User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the ″guest″ user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name
User name for the administrator

Password
Password for the administrator

Note: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name
Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name
Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

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

Root signing certificate

Expiration period in years
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
Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Deployment manager for Version 7.0

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: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZManagement*xx*	

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

Server Type Selection

Item	Default	Your value
Server type	Deployment manager	Deployment manager

Default 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	

Target Datasets

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

Configure Common Groups

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

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

Configure Common Users

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

System and Dataset Names

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

Cell, Node, and Server Names

Item	Default	Your value
Cell names		

Item		Default	Your value
	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	

Configuration File System

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 *	
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.			

WebSphere Application Server Product File System

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	

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7DCR	
Servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO7DSR	

Port Values Assignment

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	
DataPower appliance manager secure inbound port		5555	

Location Service Daemon Definitions

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	

SSL Customization

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 writable SAF keyring support	Not selected	
Enable SSL on location service daemon	Selected	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			*cell_short_name*	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

Item	Default	Your value
User name	WSADMIN	
Password	None	

Security Certificate

Item	Default	Your value
Default personal certificate		

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

Job Statement Definition

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

Customization worksheet: Deployment manager for Version 6.1

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: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZDmgr*xx*	
Response file path name (optional)	None	

Default Values

Item	Default	Your value
GID and UID defaults		

Item			Default	Your value
	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	

Target Datasets

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

Configure Common Groups

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

Configure Common Users

Item	Default	Your value
Common controller user ID		

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

Names and Dataset Qualifier

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	
Websphere product dataset high-level qualifier	None	

Product Datasets

Item	Default	Your value
SBBOLPA dataset name or catalog alias	*product_hlq*.SBBOLPA	
SBBOEXEC dataset name	*product_hlq*.SBBOEXEC	
SBBOMSG dataset name	*product_hlq*.SBBOMSG	
SBBOLOAD dataset name or catalog alias	*product_hlq*.SBBOLOAD	
SBBGLOAD dataset name or catalog alias	*product_hlq*.SBBGLOAD	
SBBOLD2 dataset name or catalog alias	*product_hlq*.SBBOLD2	
Run WebSphere Application Server from STEPLIB	Selected	

Cell, Node, and Server Names

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	

Configuration File System

Item		Default	Your value
Mount point		/wasv61config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point		DeploymentManager	
Dataset name		OMVS.WAS61.*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	

WebSphere Application Server Product File System

Item			Default	Your value
Product file system directory			/usr/lpp/zWebSphere/V6R1	
Intermediate symbolic link				
	Create intermediate symbolic link		Selected	
		Path name of intermediate symbolic link	/wasv61config/*cell_long_name*/*node_long_name*/wassmpe	

Optional Application Deployment

Item	Default	Your value
Deploy the administrative console	Selected	

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO6DCR	
Servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO6DSR	

Port Values Assignment

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	
High Availability Manager communication port (DCS)		9352	

Location Service Daemon Definitions

Item	Default	Your value
Daemon home directory	/wasv61config/ *cell_long_name*/ *node_long_name*/Daemon	/wasv61config/*cell_long_name*/ *node_long_name*/ Daemon
Daemon job name	BBODMNC	
Procedure name	BBO6DMNC	
IP name	*host_name*	
Listen IP	*	
Port	5755	

Item	Default	Your value
SSL port	5756	
Register daemon with WLM DNS	Not selected	

SSL Customization

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	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			*cell_short_name*	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

Item	Default	Your value
User name	WSADMIN	
Password	None	

Job Statement Definition

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

Item	Default	Your value
//*	//*	
//*	//*	

Planning for a new managed node in a Network Deployment cell

Before you begin

You need to have already configured a Network Deployment cell and deployment manager.

About this task

Create a new managed node in a Network Deployment cell in order to add application servers to the cell.

This part of the configuration process creates an application server node structure, a node agent (for node administration), and a location service daemon (if one does not already exist) for the chosen z/OS system. This can be the same z/OS system on which the deployment manager was configured or a different z/OS system in the same sysplex. Once the managed node is created and federated into the Network Deployment cell, add application servers using the administrative console or scripting. You can use the configuration file system and user IDs created for the managed server node for the application servers in the node as well.

1. Print a copy of “Customization worksheet: Managed (custom) node for Version 7.0” on page 168.
2. Fill out the worksheet as described in “Customization variables: Managed (custom) node.”
3. Save the worksheet for use during managed node customization.

Customization variables: Managed (custom) node

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a managed (custom) node.

During this customization task, you create a (temporary) cell configuration, a node configuration, and a (temporary) location service daemon.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Note: The cell configuration and location service daemon are temporary because they are replaced shortly after creation when the new node is federated.

The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for the future node agent and application servers.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)
Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

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

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

Name and userid defaults
Set default names and user IDs based on cell and system identifiers

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

Two-character cell identifier
Two-character cell identifier (for the Network Deployment cell into which this node will be federated) to be used to create default names and user IDs

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

Single-character system identifier
Single-character system identifier to be used to create default names and user IDs

Note: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults
Select default port values from the following port range

The port range must contain at least 10 ports.

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the servant group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID
User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
User identifier associated with the control region user ID

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

Common servant user ID

User ID
User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID
User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the administrator user ID

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

Asynchronous administrator user ID

User ID
User ID that is used to run asynchronous administration operations procedure

This user ID must be a member of the WebSphere Application Server configuration group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
UNIX System Services UID number for the asynchronous administration task user ID

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name
Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Node Names

Note: A cell short name of BBOTEMP and a cell long name of bbotemp will be assigned to the unfederated managed node. These names will no longer be used after the managed node is federated into a Network Deployment cell.

Node names

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

Note:

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

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

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

Note:

- Name must be 50 or fewer characters.
- 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.

Configuration File System

Note: The cell long name is included in the default mount point and the cell short name is included in the default dataset name. If you plan to federate this application server into a Network Deployment cell, you might want to change the cell long and short names in these default values to the actual long and short names of the cell into which this node will be federated.

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 300 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

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

Read "Product file system" on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Process Definitions

Controller process

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Controller adjunct process

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

Note: Name must be seven or fewer characters.

Servant process

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Admin asynch operations procedure name
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

Read “Cataloged procedures” on page 54 for more information.

Location Service Daemon Definitions

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
Directory in which the location service daemon resides

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

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

Note: When configuring a new node, 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
Name of the member in your procedure library to start the location service daemon

Note: Name must be seven or fewer characters.

SSL Customization

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

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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.

You might want to set the managed node's SAF key ring name to be the same as that of the Network Deployment cell into which it will be federated.

Enable writable SAF keyring support
Select this option if you want to enable writable SAF key ring support

Administrative Security Selection

Use a z/OS security product
Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server
Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

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

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security
Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Federate Application Server

Application server access

WebSphere Application Server home directory path name
Home directory

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

Directory path name relative to mount point
Relative path name of the directory within the configuration file system in which the application server configuration resides

Deployment manager access

Node host name or IP address
IP name or address of the system on which the deployment manager server is configured

This value, equivalent to ″cell host″ in addNode.sh, is used by other WebSphere Application Server for z/OS functions to connect to this server in order to federate the designated node into the deployment manager cell.

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

Deployment manager JMX connection type

RMI Connect to the deployment manager using an RMI connection

SOAP Connect to the deployment manager using a SOAP connection

Deployment manager JMX port
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 connection requires security information
Indicates whether a user ID (and associated password) with full administration privileges is required to connect to the deployment manager

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

User ID
User ID with full administrative privileges for the Network Deployment cell

Password
Password for the user ID that has full administrative privileges for the Network Deployment cell

Node agent definitions

Server name (short)
Name of the node agent server

This is the server's jobname, as specified in the MVS START command JOBNAME parameter. This value identifies the server to certain z/OS facilities used by WebSphere Application Server for z/OS (SAF for example).

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

Server name (long)
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.

Node host name
IP address or host name of the system on which the node resides

JMX SOAP connector port
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 and is invoked through scripts such as wsadmin.sh.

Note: Value cannot be 0.

ORB listener IP address
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
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

Node discovery port
Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager (NODE_DISCOVERY_ADDRESS)

Node multicast discovery port
Defines the multicast port through which the node agent sends discovery requests to its managed servers (NODE_MULTICAST_DISCOVERY_ADDRESS)

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
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
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 (DCS)
Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Node group name
Node group into which the node will be placed

Specify DefaultNodeGroup if the node is in the same sysplex as the deployment manager.

Launch the node agent after node federation
Indicates whether the node agent is to be started automatically after federating a node

Security Certificate

Default personal certificate

Issued to distinguished name
Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name
Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

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

Root signing certificate

Expiration period in years
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
Default password for all keystores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Managed (custom) node for Version 7.0

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: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZCustom*xx*	
Response file path name (optional)	None	

Default 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	

Target Datasets

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

Configure Common Groups

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

Configure Common Users

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

System and Dataset Names

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

Node Names

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

Configuration File System

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.			

WebSphere Application Server Product File System

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	

Process Definitions

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	

Location Service Daemon Definitions

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	

SSL Customization

Item	Default	Your value
Certificate authority keylabel	WebSphereCA	
Expiration date for certificates	2018/12/31	
Default SAF keyring name	WASKeyring.*cell_short_name*	
Enable writable SAF keyring support	Not selected	

Administrative Security Selection

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

Federate Application Server (Part 1)

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*	/wasv7config/*cell_long_name*/ *node_long_name*
		Directory path name relative to mount point	AppServer	AppServer
Deployment manager access				

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

Federate Application Server (Part 2)

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	2809	
		ORB SSL port	0	
	Node discovery port		7272	
	Node multicast discovery port		5000	
	Node IPv6 multicast discovery port		5001	
	Administrative local port		9629	
	High Availability Manager communication port (DCS)		9354	
Node group name			DefaultNodeGroup	
Launch the node agent after federation			Selected	

Security Certificate

Item		Default	Your value
Default personal certificate			
	Issued to distinguished name	cn=*host_name*, ou=*cell_short_name*, ou=*node_short_name*,c=IBM,c=US	
	Issued by distinguished name	cn=*host_name*, ou=Root Certificate, ou=*cell_short_name*, ou=*node_short_name*,c=IBM,c=US	
	Expiration period in years	1	
Root signing certificate			

Item		Default	Your value
	Expiration period in years	20	
Default keystore password			

Job Statement Definition

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

Customization worksheet: Managed (custom) node for Version 6.1

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: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZCustom*xx*	
Response file path name (optional)	None	

Default 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				

Item			Default	Your value
	Set default port values from the following port range		Not selected	
		Lowest default port number	9550	
		Highest default port number	9559	

Target Datasets

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

Configure Common Groups

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

Configure Common Users

Item				Default	Your value
Common controller user ID					
	User ID			WSCRU1	
		Allow OS security to assign UID		Not selected	
		Allow user-specified UID		Selected	
			Specified UID	2431	
Common servant user ID					

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

Names and Dataset Qualifier

Item	Default	Your value
System name	None	
Sysplex name	None	
PROCLIB dataset name	SYS1.PROCLIB	
Websphere product dataset high-level qualifier	None	

Product Datasets

Item	Default	Your value
SBBOLPA dataset name or catalog alias	*product_hlq*.SBBOLPA	
SBBOEXEC dataset name	*product_hlq*.SBBOEXEC	
SBBOMSG dataset name	*product_hlq*.SBBOMSG	
SBBOLOAD dataset name or catalog alias	*product_hlq*.SBBOLOAD	
SBBGLOAD dataset name or catalog alias	*product_hlq*.SBBGLOAD	
SBBOLD2 dataset name or catalog alias	*product_hlq*.SBBOLD2	
Run WebSphere Application Server from STEPLIB	Selected	

Node Names

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

Configuration File System

Item		Default	Your value
Mount point		/wasv61config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point		AppServer	
Dataset name		OMVS.WAS61.*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	

WebSphere Application Server Product File System

Item			Default	Your value
Product file system directory			/usr/lpp/zWebSphere/V6R1	
Intermediate symbolic link				
	Create intermediate symbolic link		Selected	
		Path name of intermediate symbolic link	/wasv61config/*cell_long_name*/*node_long_name*/wassmpe	

Process Definitions

Item		Default	Your value
Controller process			
	Procedure name	BBO6ACR	
Controller adjunct process			
	Procedure name	BBO6CRA	
Servant process			
	Procedure name	BBO6ASR	

Item	Default	Your value
Admin asynch operations procedure name	BBOW6SH	

Location Service Daemon Definitions

Item	Default	Your value
Daemon home directory	/wasv61config/ *cell_long_name*/ *node_long_name*/Daemon	/wasv61config/*cell_long_name*/ *node_long_name*/ Daemon
Daemon job name	BBODMNB	
Procedure name	BBO6DMN	

SSL Customization

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

Administrative Security Selection

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

Federate Application Server (Part 1)

Item			Default	Your value
Application server access				
	WebSphere Application Server home directory path name			
		Configuration file system mount point	/wasv61config/ *cell_long_name*/ *node_long_name*	/wasv61config/*cell_long_name*/ *node_long_name*
		Directory path name relative to mount point	AppServer	AppServer
Deployment manager access				

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

Federate Application Server (Part 2)

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	2809	
		ORB SSL port	0	
	Node discovery port		7272	
	Node multicast discovery port		5000	
	Node IPv6 multicast discovery port		5001	
	High Availability Manager communication port (DCS)		9354	
Node group name			DefaultNodeGroup	
Launch the node agent after federation			Selected	

Job Statement Definition

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

Planning to federate a standalone server into a Network Deployment cell

Before you begin

You must have configured a Network Deployment cell (and deployment manager) and a standalone application server. The two need to have a common MVS group and user domain and reside within the same z/OS sysplex.

About this task

Federate an existing standalone application server node into a Network Deployment cell in order to add application servers to the cell. The Deployment Manager needs to be at an equal or higher service level than the node being federated.

The cell structure and location service daemon for the standalone application server are discarded. The standalone application server node and its application servers become a new node in the Network Deployment cell. The standalone application server's configuration file system and home directory stay in use, but are modified to reflect the new cell name. New symbolic links for use during server startup are added.

1. Print a copy of "Customization worksheet: Federating an application server for Version 7.0" on page 184.
2. Fill out the worksheet as described in "Customization variables: Federating an application server."
3. Save the worksheet for use during federated application server node customization.

Customization variables: Federating an application server

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to federate an application server.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Customization Definition Name

Customization definition name
Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)
Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

Port defaults
Select default port values from the following port range

When this option is not selected, each port value defaults to an IBM-provided number. When this option is selected, each port default value is selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Federate Application Server

Application server access

WebSphere Application Server home directory path name
Home directory

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

Directory path name relative to mount point
Relative path name of the directory within the configuration file system in which the application server configuration resides

Application server security is enabled
Indicates whether global security is enabled on the cell containing the application server

User ID
User ID with full administrative privileges for the cell containing the application server

Password
Password for the user ID that has full administrative privileges for the cell containing the application server

Deployment manager access

Node host name or IP address
IP name or address of the system on which the deployment manager server is configured

This value, equivalent to ″cell host″ in addNode.sh, is used by other WebSphere Application Server for z/OS functions to connect to this server in order to federate the designated node into the deployment manager cell.

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

Deployment manager JMX connection type

RMI Connect to the deployment manager using an RMI connection

SOAP Connect to the deployment manager using a SOAP connection

Deployment manager JMX port
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 connection requires security information
Indicates whether a user ID (and associated password) with full administration privileges is required to connect to the deployment manager

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

User ID
User ID with full administrative privileges for the Network Deployment cell

Password
Password for the user ID that has full administrative privileges for the Network Deployment cell

Node agent definitions

Server name (short)
Name of the node agent server

This is the server's jobname, as specified in the MVS START command JOBNAME parameter. This value identifies the server to certain z/OS facilities used by WebSphere Application Server for z/OS (SAF for example).

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

Server name (long)
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
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 and is invoked through scripts such as wsadmin.sh.

Note: Value cannot be 0.

ORB listener IP address
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
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

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

Node discovery port
Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager (NODE_DISCOVERY_ADDRESS)

Node multicast discovery port
Defines the multicast port through which the node agent sends discovery requests to its managed servers (NODE_MULTICAST_DISCOVERY_ADDRESS)

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
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
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 (DCS)
Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Application server's new ORB port
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

This user ID also owns all of the configuration file systems.

Note: Value cannot be 0.

Node group name
Node group into which the node will be placed

Specify DefaultNodeGroup if the node is in the same sysplex as the deployment manager.

Configuration group name
Group name of the WebSphere Application Server configuration group

Configuration user ID
User ID that owns the configuration file system

Include apps
Indicates whether to include applications with your deployment manager node

Enabling this option instructs the addNode command to include applications from the node; otherwise, it would remove them prior to federation. If the application already exists in the cell, a warning is printed and the application is not installed into the cell.

You must use this option to migrate all of the applications to the new cell. Federating the node to a cell using the addNode command does not merge any cell-level configuration information, including that from virtualHost.

Launch the node agent after node federation
Indicates whether the node agent is to be started automatically after federating a node

Federate service integration busses that exist on this node
Indicates whether to federate service integration busses that exist on this node

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Customization worksheet: Federating an application server for Version 7.0

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 federated node:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZFederate*xx*	
Response file path name (optional)	None	

Default Values

Item			Default	Your value
Port defaults				
	Set default port values from the following port range		Not selected	
		Lowest default port number	9550	
		Highest default port number	9559	

Target Datasets

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

Federate Application Server (Part 1)

Item			Default	Your value
Application server access				
	WebSphere Application Server home directory path name			
		Configuration file system mount point	/wasv7config	
		Directory path name relative to mount point	AppServer	
	Application server security is enabled		Not selected	
		Local user ID	None	
		Local password	None	
Deployment manager access				

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

Federate Application Server (Part 2)

Item			Default	Your value
Node agent definitions				
	Server name (short)		BBON001	
	Server name (long)		nodeagent	nodeagent
	JMX SOAP connector port		8878	
	ORB listener IP address		*	
		ORB port	2809	
		ORB SSL port	0	
	Node discovery port		7272	
	Node multicast discovery port		5000	
	Node IPv6 multicast discovery port		5001	
	Administrative local port		9629	
	High Availability Manager communication port (DCS)		9354	
Application server's new ORB port			9810	
Node group name			DefaultNodeGroup	
Configuration group name			WSCFG1	
Configuration user ID			WSADMIN	
Include apps			Selected	
Launch the node agent after federation			Selected	
Federate service integration busses that exist on the node			Not selected	

Job Statement Definition

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

Customization worksheet: Federating an application server for Version 6.1

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 federated node:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZFederate*xx*	
Response file path name (optional)	None	

Default Values

Item			Default	Your value
Port defaults				
	Set default port values from the following port range		Not selected	
		Lowest default port number	9550	
		Highest default port number	9559	

Target Datasets

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

Federate Application Server (Part 1)

Item	Default	Your value
Application server access		

Item			Default	Your value
	WebSphere Application Server home directory path name			
		Configuration file system mount point	/wasv61config	
		Directory path name relative to mount point	AppServer	
	Application server security is enabled		Not selected	
		Local user ID	None	
		Local password	None	
Deployment manager access				
	Node host name or IP address		None	
	Deployment manager JMX connection type			
		RMI	Not selected	
		SOAP	Selected	
	Deployment manger JMX port		8879	
	Deployment manager connection requires security information		Not selected	
		User ID	WSADMIN	
		Password	None	

Federate Application Server (Part 2)

Item			Default	Your value
Node agent definitions				
	Server name (short)		BBON001	
	Server name (long)		nodeagent	nodeagent
	JMX SOAP connector port		8878	
	ORB listener IP address		*	
		ORB port	2809	
		ORB SSL port	0	
	Node discovery port		7272	
	Node multicast discovery port		5000	
	Node IPv6 multicast discovery port		5001	
	High Availability Manager communication port (DCS)		9354	
Application server's new ORB port			9810	
Node group name			DefaultNodeGroup	
Configuration group name			WSCFG1	
Configuration user ID			WSADMIN	
Include apps			Selected	
Launch the node agent after federation			Selected	
Federate service integration busses that exist on the node			Not selected	

Job Statement Definition

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

Planning for a Network Deployment cell with an application server

About this task

A Network Deployment cell is a full-function WebSphere Application Server for z/OS configuration on which you can deploy and run applications. A Network Deployment cell with application server includes the following:

- Cell configuration
- Deployment manager that runs the administrative console application
- Single location service daemon on each z/OS system
- One application server consisting of a node agent and one application server
- One or more application server nodes (one is recommended) on each z/OS target system hosting portions of the cell. Each node consists of a node agent and some number of application servers

This part of the configuration process creates the initial cell configuration, the deployment manager, and a location service daemon for the z/OS system, plus a node agent with an application server. Once the Network Deployment cell is created, you can add additional application server nodes by creating and federating new managed nodes, or by federating standalone application server nodes into the Network Deployment cell.

When configuring your deployment manager node, set up your file system such that the root file system is shared among all processors and the deployment manager's configuration is in a configuration file system on a system-generic mount point.

Note: This configuration scenario is the best for certain tasks, such as starting the deployment manager on another system, that you might want to perform in the future.

1. Print a copy of "Customization worksheet: Network Deployment cell with an application server for Version 7.0" on page 207.
2. Fill out the worksheet as described in "Customization variables: Network Deployment cell with an application server."
3. Save the worksheet for use during Network Deployment cell with an application server customization.

Customization variables: Network Deployment cell with an application server

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a Network Deployment cell with an application server.

The WebSphere Application Server for z/OS runtime requires four standalone cell servers: application server, deployment manager, node agent, and location service daemon. The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for a Network Deployment cell with an application server.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name
Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)
Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

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

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

Name and userid defaults
Set default names and user IDs based on cell, cluster, and system identifiers

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

Two-character cell identifier
Two-character cell identifier to be used to create default names and user IDs

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

Two-character cluster identifier
Two-character cluster identifier to be used to create default names and user IDs

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

Single-character system identifier
Single-character system identifier to be used to create default names and user IDs

Note: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults
Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 50 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the servant group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID

User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Allow user-specified UID

Select this option to specify a specific UID value.

Specified UID

User identifier associated with the control region user ID

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

Common servant user ID

User ID

User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Allow user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID

User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Allow user-specified UID

Select this option to allow to allow a user-specified ID.

Specified UID

User identifier associated with the administrator user ID

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

Asynchronous administrator user ID

User ID

User ID that is used to run asynchronous administration operations procedure

This user ID must be a member of the WebSphere Application Server configuration group.

Allow OS security to assign UID

Select this option to have RACF assign an unused UID value.

Allow user-specified UID

Select this option to specify a specific UID value.

Specified UID

UNIX System Services UID number for the asynchronous administration task user ID

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

WebSphere Application Server user ID home directory

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

System name

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

Sysplex name

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name

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

Cell, Node, and Server Names

Cell names

Short name

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

Note:

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

Long name

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

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

Note:

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

Deployment manager node names

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

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

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

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

Note:
- Name must be 50 or fewer characters.
- 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.

Deployment manager server names

Short name
Name that identifies the server to z/OS facilities such as SAF

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

Long name
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.

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

Node agent and application server node names

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

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

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

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

Note:
- Name must be 50 or fewer characters.
- 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.

Node agent server names

Short name
Name that identifies the server to z/OS facilities such as SAF

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

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

Long name
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.

Note: Name must be 50 or fewer characters.

Application server names

Short name
Name that identifies the server to z/OS facilities such as SAF

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

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

Long name
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.

Note: Name must be 50 or fewer characters.

Deployment manager cluster transition name
WLM APPLENV (WLM application environment) name for the deployment manage

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. See “Cataloged procedures” on page 54 for more information.

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

Application server cluster transition name
WLM APPLENV (WLM application environment) name for the application server

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. See “Cataloged procedures” on page 54 for more information.

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

JVM mode

31 bit Specifies that the JVM in each application server is to run in 31-bit mode

64 bit Specifies that the JVM in each application server is to run in 64-bit mode

Deployment Manager Configuration File System

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

Deployment Manager Product File System

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

Read "Product file system" on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Application Server Configuration File System

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

Application Server Product File System

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

Read "Product file system" on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Optional Application Deployment

Deploy the administrative console
Specify whether to install a Web-based administrative console that manages the application server.

Deploying the administrative console is recommended, but if you deselect this option, the information center contains detailed steps for deploying it after the profile exists.

Deploy the default application
Specify whether to install the default application that contains the Snoop, Hello, and HitCount servlets.

Deploy the sample applications
Specify whether to install the sample applications (the Samples Gallery).

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.

Process Definitions

Deployment manager controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Deployment manager servant process

Job name
Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter ″S″, and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Application server controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Application server controller adjunct process

Job name
Job name used by WLM to start the application server control region adjunct

This is set to the server short name followed by the letter ″A″, and it cannot be changed through the tool.

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

Note: Name must be seven or fewer characters.

Application server servant process

Job name
Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter ″S″, and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Admin asynch operations procedure name
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

Read “Cataloged procedures” on page 54 for more information.

Port Values Assignment

Deployment manager ports:

Node host name or IP address
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.

JMX SOAP connector port
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.

Note: Value cannot be 0.

Cell discovery address port
Port number used by node agents to connect to this deployment manager server (CELL_DISCOVERY_ADDRESS)

ORB listener IP address
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
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

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

HTTP transport IP address
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. 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
Port for HTTP requests to the administrative console

Administrative console secure port
Port for secure HTTP requests to the administrative console

Administrative interprocess communication port (K)
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 (DCS)
Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Note: Value cannot be 0.

DataPower appliance manager secure inbound port
Port used to receive events from DataPower appliances that are managed by the DataPower appliance manager (DataPowerMgr_inbound_secure)

Node agent ports:

JMX SOAP connector port
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.

Note: Value cannot be 0.

ORB port
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

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

Node agent interprocess communication port (K)
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 (DCS)
Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Note: Value cannot be 0.

Node discovery port
Defines the TCP/IP port to which the node agents listens for discovery requests that originate from the deployment manager (NODE_DISCOVERY_ADDRESS)

Node multicast discovery port
Defines the multicast port through which the node agent sends discovery requests to its managed servers (NODE_MULTICAST_DISCOVERY_ADDRESS)

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
Defines the IPv6 multicast port through which the node agent sends discovery requests to its managed servers (NODE_IPV6_MULTICAST_DISCOVERY_ADDRESS)

Application server ports:

JMX SOAP connector port
Port number for the JMX HTTP connection to this server based on the SOAP protocol protocol (SOAP_CONNECTOR_ADDRESS)

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

Note: Value cannot be 0.

ORB port
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

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

HTTP transport port
Port for HTTP requests (WC_defaulthost)

Note: Value cannot be 0.

HTTPS transport port
Port for secure HTTP requests (WC_defaulthost_secure)

Note: Value cannot be 0.

Administrative local port
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 (DCS)
Port on which the High Availability Manager listens (DCS_UNICAST_ADDRESS)

Note: Value cannot be 0.

Service integration port
Port for service-integration requests (SIB_ENDPOINT_ADDRESS)

Note: Value cannot be 0.

Service integration secure port
Port for secure service-integration requests (SIB_ENDPOINT_SECURE_ADDRESS)

Note: Value cannot be 0.

Service integration MQ interoperability port
Port for service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_ADDRESS)

Note: Value cannot be 0.

Service integration MQ interoperability secure port
Port for secure service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_SECURE_ADDRESS)

Note: Value cannot be 0.

Session initiation protocol (SIP) port
Port for session initiation requests (SIP_DEFAULTHOST)

Note: Value cannot be 0.

Session initiation protocol (SIP) secure port
Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Note: Value cannot be 0.

Location Service Daemon Definitions

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
Directory in which the location service daemon resides

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

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

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

Note: Name must be seven or fewer characters.

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

The default value 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.

Listen IP
Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

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

Register daemon with WLM DNS
If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

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

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

Generate certificate authority (CA) certificate
Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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
Select this option if you want to enable writable SAF key ring support

Enable SSL on location service daemon
Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

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

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

Internally, this sets ″SecurityDomainType″ to the string ″cellQualified″. All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the ″guest″ user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name
User name for the administrator

Password
Password for the administrator

Note: This password must not be blank.

Specify a user name and password to login to the Samples user account.

Sample applications

User name
User name for the samples user account

Password
Password for the samples user account

Security Certificate

Default personal certificate

Issued to distinguished name
Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name
Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

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

Root signing certificate

Expiration period in years
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
Default password for all keystores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Web Server Definition

Create a Web server definition
Indicates whether to create a Web server definition.

Web server type
Select the Web server type from the list of supported Web servers.

Web server operating system
Operating system where the Web server is located

Web server name
Name used in defining the Web server to WebSphere Application Server

Web server host name or IP address
IP name or address of the system on which the Web server is located

Web server port
HTTP port on which the Web server listens

Web server installation directory path
Name of the directory where the Web server is installed

Web server plug-in installation directory path
Name of the directory in where the Web server plug-ins are installed

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Network Deployment cell with an application server for Version 7.0

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 Network Deployment cell:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZCell*xx*	
Response file path name (optional)	None	

Default 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	9530	
		Highest default port number	9549	

Target Datasets

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

Configure Common Groups

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

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

Configure Common Users

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

System and Dataset Names

Item	Default	Your value
System name	None	
Sysplex name	None	

Item	Default	Your value
PROCLIB dataset name	SYS1.PROCLIB	

Cell, Node, and Server Names

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	dmgr
Node agent and application server node names			
	Short name	BBONODE	
	Long name	bbonode	
Node agent server names			
	Short name	BBON001	
	Long name	nodeagent	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	

Deployment Manager Configuration File System

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*	
File system type		

Item		Default	Your value
	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.			

Deployment Manager Product File System

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	

Application Server Configuration File System

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	

Application Server Product File System

Item	Default	Your value
Product file system directory	/usr/lpp/ zWebSphere/ V7R0	

Item			Default	Your value
Intermediate symbolic link				
	Create intermediate symbolic link		Selected	
		Path name of intermediate symbolic link	/wasv7config/*cell_long_name*/*nodeagent_long_name*wassmpe	

Optional Application Deployment

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

Process Definitions

Item		Default	Your value
Deployment manager controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7DCR	
Deployment manager servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO7DSR	
Application server controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7ACR	
Application server controller adjunct process			
	Job name	*server_short_name*A	*server_short_name*A
	Procedure name	BBO7CRA	
Application server servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO7ASR	
Admin asynch operations procedure name		BBO7ADM	

Port Values Assignment

Item	Default	Your value
Deployment manager ports		
Node host name or IP address	None	

Item		Default	Your value
	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		5555	
Node agent ports			
JMX SOAP connector port		8878	
ORB port		2809	
ORB SSL port		0	
Node agent interprocess communication port (K)		9629	
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	
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	

Item	Default	Your value
Session initiation protocol (SIP) secure port	5061	

Location Service Daemon Definitions

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	

SSL Customization

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 writable SAF keyring support	Not selected	
Enable SSL on location service daemon	Selected	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item	Default	Your value
SAF profile prefix	*cell_short_name*	
WebSphere Application Server unauthenticated user		

Item			Default	Your value
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

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

Security Certificate

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

Web Server Definition (Part 1)

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	*host_name*	
	Web server port	80	

Web Server Definition (Part 2)

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

Job Statement Definition

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

Customization worksheet: Network Deployment cell with an application server for Version 6.1

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 Network Deployment cell:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZCell*xx*	
Response file path name (optional)	None	

Default 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			

Item			Default	Your value
	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	9530	
		Highest default port number	9549	

Target Datasets

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

Configure Common Groups

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

Configure Common Users

Item	Default	Your value
Common controller user ID		

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

Names and Dataset Qualifier

Item	Default		Your value
System name	None		
Sysplex name	None		
PROCLIB dataset name	SYS1.PROCLIB		
Websphere product dataset high-level qualifier for the deployment manager	None		
Websphere product datasets for the application server			
	Use same product dataset names as deployment manager	Selected	
	Use different product dataset names than deployment manager	Not selected	
	High-level qualifier	None	

Product Datasets

Item	Default	Your value
SBBOLPA dataset name or catalog alias	*product_hlq*.SBBOLPA	
SBBOEXEC dataset name	*product_hlq*.SBBOEXEC	
SBBOMSG dataset name	*product_hlq*.SBBOMSG	
SBBOLOAD dataset name or catalog alias	*product_hlq*.SBBOLOAD	
SBBGLOAD dataset name or catalog alias	*product_hlq*.SBBGLOAD	
SBBOLD2 dataset name or catalog alias	*product_hlq*.SBBOLD2	
Run WebSphere Application Server from STEPLIB	Selected	

Cell, Node, and Server Names

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	dmgr
Node agent and application server node names			
	Short name	BBONODE	
	Long name	bbonode	
Node agent server names			
	Short name	BBON001	
	Long name	nodeagent	nodeagent
Application server names			
	Short name	BBOS001	
	Long name	server1	
Deployment manager cluster transition name		BBODMGR	
Application server cluster transition name		BBOC001	

Deployment Manager Configuration File System

Item	Default	Your value
Mount point	/wasv61config/ *cell_long_name*/ *node_long_name*	

Item		Default	Your value
Directory path name relative to mount point		DeploymentManager	
Dataset name		OMVS.WAS61.*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	

Deployment Manager Product File System

Item			Default	Your value
Product file system directory			/usr/lpp/zWebSphere/V6R1	
Intermediate symbolic link				
	Create intermediate symbolic link		Selected	
		Path name of intermediate symbolic link	/wasv61config/*cell_long_name*/*node_long_name*/wassmpe	

Application Server Configuration File System

Item		Default	Your value
Mount point		/wasv61config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point		AppServer	
Dataset name		OMVS.WAS61.*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	

Application Server Product File System

Item			Default	Your value
Product file system directory			/usr/lpp/zWebSphere/V6R1	
Intermediate symbolic link				
	Create intermediate symbolic link		Selected	
		Path name of intermediate symbolic link	/wasv61config/*cell_long_name*/*nodeagent_long_name*wassmpe	

Optional Application Deployment

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

Process Definitions

Item		Default	Your value
Deployment manager controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO6DCR	
Deployment manager servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO6DSR	
Application server controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO6ACR	
Application server controller adjunct process			
	Job name	*server_short_name*A	*server_short_name*A
	Procedure name	BBO6CRA	
Application server servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO6ASR	
Admin asynch operations procedure name		BBOW6SH	

Port Values Assignment

Item	Default	Your value
Deployment manager ports		

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	
High Availability Manager communication port (DCS)		9352	
Node agent ports			
JMX SOAP connector port		8878	
ORB port		2809	
ORB SSL port		0	
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	
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	

Location Service Daemon Definitions

Item	Default	Your value
Daemon home directory	/wasv61config/ *cell_long_name*/ *dngr_node_long_name*/ Daemon	/wasv61config/*cell_long_name*/ *dngr_node_long_name*/ Daemon
Daemon job name	BBODMNC	
Procedure name	BBO6DMN	
IP name	*host_name*	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

SSL Customization

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	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			*cell_short_name*	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

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

Web Server Definition (Part 1)

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	*host_name*	
	Web server port	80	

Web Server Definition (Part 2)

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

Job Statement Definition

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

Planning for a job manager

A job manager allows you to submit administrative jobs asynchronously for application servers registered to administrative agents and for deployment managers. You can submit these jobs to a large number of servers over a geographically dispersed area.

About this task

You can make the following types of servers known to a job manager through a registration process:

- Application servers registered to administrative agents

You can register standalone application server nodes with an administrative agent. You can then register one or more of the nodes with a job manager.

- Deployment managers

After you register the servers, you can queue administrative jobs directed at the application servers or deployment managers through the job manager.

The job manager allows you to asynchronously administer job submissions. You can perform the following tasks:

- Set a job submission to take effect at a specified time.
- Set a job submission to expire at a specified time.
- Schedule a job submission to occur at a specified time interval.
- Notify the administrator through e-mail that a job has completed.

For more information, read the ″Administering nodes using the job manager″ article in the information center.

1. Print a copy of “Customization worksheet: Job manager” on page 237.
2. Fill out the worksheet as described in “Customization variables: Job manager.”
3. Save the worksheet for use during job manager customization.

Customization variables: Job manager

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a job manager.

The WebSphere Application Server for z/OS runtime requires four servers in a Network Deployment cell: application server, deployment manager, node agent, and location service daemon. The customization corresponding to the following sections sets up the names, network configuration, start procedures, and user IDs for a deployment manager.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the

same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Server Type Selection

Server type
Type of server to be created within this management profile

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read "Configuration Planning Spreadsheet for z/OS" on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

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

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

Name and userid defaults
Set default names and user IDs based on a cell and system identifiers

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

Two-character cell identifier
Two-character cell identifier to be used to create default names and user IDs

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

Single-character system identifier
Single-character system identifier to be used to create default names and user IDs

Note: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults
Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the servant group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID
User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
User identifier associated with the control region user ID

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

Common servant user ID

User ID
User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID
User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the administrator user ID

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

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name
Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

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

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

Note:

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

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

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

Note:

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

Node names

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

Note:

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

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

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

Note:

- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names

Short name
Name that identifies the server to z/OS facilities such as SAF

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

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

Long name
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.

Note: Name must be 50 or fewer characters.

Cluster transition name
WLM APPLENV (WLM application environment) name for this server

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. See “Cataloged procedures” on page 54 for more information.

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

Configuration File System

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

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

This is the SMP/E installation directory.

Read "Product file system" on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Process Definitions

Controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Servant process

Job name
Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter ″S″, and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address
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.

JMX SOAP connector port
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.

Note: Value cannot be 0.

ORB listener IP address
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
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)

Note: Value cannot be 0.

ORB SSL port
Port for secure IIOP requests (ORB_SSL_LISTENER_ADDRESS)

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

HTTP transport IP address
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. 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
Port for HTTP requests to the administrative console (WC_adminhost)

Administrative console secure port
Port for secure HTTP requests to the administrative console (WC_adminhost_secure)

Administrative interprocess communication port (K)
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).

Location Service Daemon Definitions

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
Directory in which the location service daemon resides

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

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

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

Note: Name must be seven or fewer characters.

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

The default value 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.

Listen IP
Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

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

Register daemon with WLM DNS
If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

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

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

Generate certificate authority (CA) certificate
Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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
Select this option if you want to enable writable SAF key ring support

Enable SSL on location service daemon
Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product

Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server

Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

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

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security

Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Security Managed by the z/OS Product

SAF profile prefix (optional)

SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID

User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the ″guest″ user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name
User name for the administrator

Password
Password for the administrator

Note: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name
Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name
Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

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

Root signing certificate

Expiration period in years
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
Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Job manager

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 job manger:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZManagement*xx*	
Response file path name (optional)	None	

Server Type Selection

Item	Default	Your value
Server type	Deployment manager	Job manager

Default 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			

Item			Default	Your value
	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	9510	
		Highest default port number	9519	

Target Datasets

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

Configure Common Groups

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

Configure Common Users

Item	Default	Your value
Common controller user ID		

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

System and Dataset Names

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

Cell, Node, and Server Names

Item		Default	Your value
Cell names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Node names			
	Short name	BBOJMGR	
	Long name	bbojmgr	
Server names			
	Short name	BBOJMGR	
	Long name	jobmgr	jobmgr
Cluster transition name		BBOJMGR	

Configuration File System

Item		Default	Your value
Mount point		/wasv7config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point		JobManager	
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	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.			

WebSphere Application Server Product File System

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	

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7JCR	
Servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO7JSR	

Port Values Assignment

Item	Default	Your value
Node host name or IP address	None	

Item		Default	Your value
	JMX SOAP connector port	8876	
ORB listener IP address		*	
	ORB port	9808	
	ORB SSL port	0	
HTTP transport IP address		*	
	Administrative console port	9960	
	Administrative console secure port	9943	
Administrative interprocess communication port (K)		9631	

Location Service Daemon Definitions

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	BBODMNJ	
Procedure name	BBO7DMNJ	
IP name	*host_name*	
Listen IP	*	
Port	5855	
SSL port	5856	
Register daemon with WLM DNS	Not selected	

SSL Customization

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 writable SAF keyring support	Not selected	
Enable SSL on location service daemon	Selected	

Administrative Security Selection

Item	Default	Your value
Use a z/OS security product	Selected	

Item	Default	Your value
Use WebSphere Application Server	Not selected	
Do not enable security	Not selected	

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			*cell_short_name*	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

Item	Default	Your value
User name	WSADMIN	
Password	None	

Security Certificate

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

Job Statement Definition

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

Planning for a secure proxy server

You can create a secure proxy server on a node in a demilitarized zone (DMZ). The DMZ zone is a safe zone between firewalls that is typically located between the client and the backend server.

1. Print a copy of “Customization worksheet: Secure proxy server” on page 254.
2. Fill out the worksheet as described in “Customization variables: Secure proxy server.”
3. Save the worksheet for use during secure proxy server customization.

Customization variables: Secure proxy server

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a secure proxy server.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

GID and UID defaults

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

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

Name and userid defaults
Set default names and user IDs based on cell and system identifiers

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

Two-character cell identifier
Two-character cell identifier to be used to create default names and user IDs

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

Single-character system identifier
Single-character system identifier to be used to create default names and user IDs

Note: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults
Select default port values from the following port range

When this option is not selected, each port value defaults to an IBM-provided number. When this option is selected, each port default value is selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

High-level qualifier (HLQ)
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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs (provides minimal access to the cell)

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID
User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
User identifier associated with the control region user ID

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

Common servant user ID

User ID
User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID
User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the administrator user ID

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

Asynchronous administration user ID
User ID used to run asynchronous administration operations procedure

It must be a member of the WebSphere Application Server configuration group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID

UNIX System Services UID number for the asynchronous administration task user ID.

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

WebSphere Application Server user ID home directory

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

System name

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

Sysplex name

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name

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

Cell, Node, and Server Names

Cell names

Short name

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

Note:

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

Long name

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

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

Note:

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

Node names

Short name

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

Note:

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

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

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

Note:
- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names

Short name
Name that identifies the server to z/OS facilities such as SAF

The server short name is also used as the server job name.

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

Long name
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.

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

Cluster transition name
WLM APPLENV (WLM application environment) name for this server

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. See “Cataloged procedures” on page 54 for more information.

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

Configuration File System

Note: The cell long name is included in the default mount point and the cell short name is included in the default dataset name. You might want to change the cell long and short names in these default values to the actual long and short names of the cell into which this node will be federated.

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

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

This is the SMP/E installation directory.

Read "Product file system" on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Process Definitions

Controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Admin asynch operations procedure name
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

Read “Cataloged procedures” on page 54 for more information.

Security Level Selection

Select the security level setting for this proxy server and choose the protocols to support.

Proxy security level

High Represents the highest level of proxy server security based on certain proxy server settings

Medium
Represents the mid-level of proxy server security based on certain proxy server settings

Low Represents the lowest level of proxy server security based on certain proxy server settings

Supported protocols

Web Select to support Web protocol

SIP Select to support SIP protocol

Port Values Assignment

Node host name or IP address
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 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.

Bootstrap port
Port for IIOP requests that acts as the bootstrap port for this server

Note: Value cannot be 0.

HTTP transport IP address
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.

HTTP transport port
Port for HTTP requests (WC_defaulthost)

Note: Value cannot be 0.

HTTPS transport port
Port for secure HTTP requests (WC_defaulthost_secure)

Note: Value cannot be 0.

Session initiation protocol (SIP) port
Port for session initiation requests (SIP_DEFAULTHOST)

Note: Value cannot be 0.

Session initiation protocol (SIP) secure port
Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Note: Value cannot be 0.

Administrative interprocess communication port (K)
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).

Location Service Daemon Definitions

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 enterprise beans for example) establish connections to the location service daemon first, then forward them to the target server.

Daemon home directory
Directory in which the location service daemon resides

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

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

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

Note: Name must be seven or fewer characters.

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

The default value 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.

Listen IP
Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

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

Register daemon with WLM DNS
If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it; otherwise, do not select it.

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

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

Generate certificate authority (CA) certificate
Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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
Select this option if you want to enable writable SAF key ring support

Enable SSL on location service daemon
Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product
Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server
Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

- A simple file-based user registry will be built as part of the customization process.

- Application-specific role bindings will be used to control role-based authorization.
- The WebSphere Application Server console users and groups list will control administrative authority.
- Digital certificates will be stored in the configuration file system as keystores.

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security
Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Security Managed by the z/OS Product

SAF profile prefix (optional)
SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID
User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the ″guest″ user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name
User name for the administrator

Password
Password for the administrator

Note: This password must not be blank.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Secure proxy server

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 secure proxy server:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZProxy*xx*	
Response file path name (optional)	None	

Default 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			

Item			Default	Your value
	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	9520	
		Highest default port number	9529	

Target Datasets

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

Configure Common Groups

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

Configure Common Users

Item				Default	Your value
Common controller user ID					
	User ID			WSCRU1	
		Allow OS security to assign UID		Not selected	
		Allow user-specified UID		Selected	
			Specified UID	2431	
Common servant user ID					

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

System and Dataset Names

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

Cell, Node, and Server Names

Item		Default	Your value
Cell names			
	Short name	BBOPROX	
	Long name	bboprox	
Node names			
	Short name	BBOPROX	
	Long name	bboprox	
Server names			
	Short name	BBOPROX	
	Long name	proxy01	
Cluster transition name		BBOPROX	

Configuration File System

Item		Default	Your value
Mount point		/wasv7config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point		SecureProxy	
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	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.			

WebSphere Application Server Product File System

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

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7XCR	
Admin asynch operations procedure name		BBO7ADM	

Security Level Selection

Item		Default	Your value
Proxy security level			
	High	Selected	
	Medium	Not selected	
	Low	Not selected	

Item		Default	Your value
Supported protocols			
	Web	Selected	
	SIP	Selected	

Port Values Assignment

Item		Default	Your value
Node host name or IP address		None	
	Bootstrap port	2809	
HTTP transport IP address		*	
	HTTP transport port	80	
	HTTPS transport port	443	
Session initiation protocol (SIP) port		5060	
Session initiation protocol (SIP) secure port		5061	
Administrative interprocess communication port (K)		9633	

Location Service Daemon Definitions

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	BBODMNX	
Procedure name	BBO7DMNX	
IP name	*host_name*	
Listen IP	*	
Port	5655	
SSL port	5656	
Register daemon with WLM DNS	Not selected	

SSL Customization

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 writable SAF keyring support	Not selected	
Enable SSL on location service daemon	Selected	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			None	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

Item	Default	Your value
User name	WSADMIN	
Password	None	

Job Statement Definition

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

Planning for a secure proxy administrative agent

A secure proxy administrative agent provides a single interface to administer multiple secure proxy servers.

About this task

An administrative agent can monitor and control multiple servers on one or more nodes. By using a single interface to administer your servers, you reduce the overhead of running administrative services in every server.

Use the following commands to register and unregister a node with the administrative agent:

- registerNode

Run the registerNode command to register a node with the administrative agent. When you run the command, the standalone node is converted into a node that the administrative agent manages. The administrative agent and the node being registered must be on the same system. You can only run the command on an unfederated node. If the command is run on a federated node, the command exits with an error.

Any node registered with the administrative agent automatically becomes eligible to register with the job manager.

- deregisterNode

  Use the deregisterNode command to deregister a node from an administrative agent so that you can use the node standalone or register the node with another administrative agent. The node must have been previously registered with the administrative agent. When you deregister a node, the node configuration is retained but is marked as not registered with the administrative agent.

An administrative agent can register any of the profiles that it manages with a job manager.

For more information, read the ″Administering nodes using the administrative agent″ article in the information center.

1. Print a copy of “Customization worksheet: Secure proxy administrative agent” on page 271.
2. Fill out the worksheet as described in “Customization variables: Secure proxy administrative agent.”
3. Save the worksheet for use during secure proxy administrative agent customization.

Customization variables: Secure proxy administrative agent

Specify values for the variables in the Profile Management Tool to create customization data and instructions that you can use to configure a secure proxy administrative agent.

The Profile Management Tool creates customization data and instructions that are used to configure a WebSphere Application Server for z/OS runtime environment. A z/OS runtime profile is neither created nor augmented, however, until the actions listed in the generated instructions are performed on the target z/OS system.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Customization Definition Name

Customization definition name

Name that identifies the customization definition

This name is used on the workstation to identify the customization data and instructions that are created. The name chosen has no effect on the WebSphere Application Server for z/OS configuration.

Response file path name (optional)

Full path name of a response file that contains the default values to be used

When this value is specified, the input fields are preloaded with the values in the response file.

Note: A response file is written each time that a customization definition is created. This response file contains all of the variable data that was used to create the customization definition, and it can be used to preload the default values when defining a similar customization definition. Normally, you should specify a response file from a customization definition of the same type as the definition that you are about to define; however, you can use a response file of a different customization-definition type to preload most of the default values for a similar type.

Default Values

Options for generating default values for this customization definition

The default values that are generated are similar to those generated by the *Configuration Planning Spreadsheet*. Read “Configuration Planning Spreadsheet for z/OS” on page 79 for more information.

If you specified a response file for setting default values, any default selected here will override the corresponding response file values.

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

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

Name and userid defaults
Set default names and user IDs based on cell and system identifiers

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

Two-character cell identifier
Two-character cell identifier to be used to create default names and user IDs

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

Single-character system identifier
Single-character system identifier to be used to create default names and user IDs

Note: The character must be an alphanumeric character. An alphabetic character can be entered in lowercase or uppercase. The case of the alphabetic character will be adjusted as appropriate for each generated default value.

Port defaults
Select default port values from the following port range

When this option is not selected, each port value will default to an IBM-provided number. When this option is selected, each port default value will be selected from the following port number range.

The port range must contain at least 10 ports.

Lowest default port number
Lowest number that may be assigned as a default port number

Highest default port number
Highest number that may be assigned as a default port number

Target Datasets

Note: The customization jobs for creating an administrative agent, deployment manager, and job manager have the same names. This means that a given pair of target datasets can only accommodate the customization jobs for a single administrative agent, deployment manager, or job manager.

High-level qualifier (HLQ)

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 is it 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.

Note: 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

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

Configure Common Groups

WebSphere Application Server configuration group information

Group Default group name for the WebSphere Application Server administrator user ID and all server user IDs

Allow OS security to assign GID

Select this option to have RACF assign an unused GID value.

Allow user-specified GID

Select this option to specify a GID value.

Specified GID

UNIX System Services GID number for the WebSphere Application Server configuration group

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

WebSphere Application Server servant group information

Group Connect all servant user IDs to this group

You can use this group to assign subsystem permissions, such as DB2 authorizations, to all servants in the security domain.

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the servant group

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

WebSphere Application Server local user group information

Group Group of local clients and unauthorized user IDs

Allow OS security to assign GID
Select this option to have RACF assign an unused GID value.

Allow user-specified GID
Select this option to specify a GID value.

Specified GID
UNIX System Services GID number for the local user group

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

Configure Common Users

Common controller user ID

User ID
User ID associated with all the control regions and the daemon

This user ID will also own all of the configuration file systems.

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

Specified UID
User identifier associated with the control region user ID

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

Common servant user ID

User ID
User ID associated with the servant and control adjunct regions

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

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the servant region user ID

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

WebSphere Application Server administrator

User ID
User ID of the initial WebSphere Application Server administrator

It must have the WebSphere Application Server configuration group as its default UNIX System Services group.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to allow to allow a user-specified ID.

Specified UID
User identifier associated with the administrator user ID

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

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

This directory does not need to be shared among z/OS systems in a WebSphere Application Server cell.

System and Dataset Names

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

Note: If you are not sure what the system name (&SYSNAME) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

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

Note: If you are not sure what the sysplex name (&SYSPLEX) is, use the console command `D SYMBOLS` on the target z/OS system to display it.

PROCLIB dataset name
Existing procedure library where the WebSphere Application Server for z/OS cataloged procedures are added

Cell, Node, and Server Names

Cell names

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

Note:

- Name must be eight or fewer characters and all uppercase.

- Name must be unique among all other cells in the sysplex.

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

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

Note:
- Name must be 50 or fewer characters.
- Name must be unique among all other cells in the sysplex.

Node names

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

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

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

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

Note:
- Name must be 50 or fewer characters.
- Name must be unique within the cell.

Server names

Short name
Name that identifies the server to z/OS facilities such as SAF

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

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

Long name
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.

Note: Name must be 50 or fewer characters.

Cluster transition name
WLM APPLENV (WLM application environment) name for this server

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. See “Cataloged procedures” on page 54 for more information.

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

Configuration File System

Mount point
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
Relative path name of the directory within the configuration file system in which the configuration resides

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

Note: You can specify up to 44 characters for the dataset name.

File system type
Type of file system that will be used when creating the WebSphere for z/OS configuration file system

Hierarchical File System (HFS)
This will allocate and mount your configuration file system dataset using HFS.

zSeries File System (ZFS)
This will allocate and mount your configuration file system dataset using ZFS.

Volume, or '*' for SMS
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
Initial size allocation in cylinders for the configuration file system dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders
Size of each secondary extent in cylinders

Note: The minimum suggested size is 100 cylinders.

WebSphere Application Server Product File System

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

This is the SMP/E installation directory.

Read "Product file system" on page 32 for more information.

Intermediate symbolic link
Select this option to allow 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.

Selecting this option will allow you to specify the path name of an intermediate symbolic link. This link will be created by the customization jobs, pointing to the product file system directory.

Path name of intermediate symbolic link
Path name of intermediate symbolic link

Process Definitions

Controller process

Job name
Job name, specified in the MVS START command JOBNAME parameter, associated with the control region

This is the same as the server short name and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the control region

Note: Name must be seven or fewer characters.

Servant process

Job name
Job name used by WLM to start the servant regions

This is set to the server short name followed by the letter ″S″, and it cannot be changed through the tool.

Procedure name
Name of member in your procedure library to start the servant regions

Note: Name must be seven or fewer characters.

Port Values Assignment

Node host name or IP address
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.

JMX SOAP connector port
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.

Note: Value cannot be 0.

Bootstrap port
Port for IIOP requests that acts as the bootstrap port for this server (BOOTSTRAP_ADDRESS)

Note: Value cannot be 0.

Administrative interprocess communication port (K)
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).

Location Service Daemon Definitions

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
Directory in which the location service daemon resides

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

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

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

Note: Name must be seven or fewer characters.

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

The default value 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.

Listen IP
Address at which the daemon listens

Select either * or a dotted decimal IP address for this value.

The default value is *.

Choose the value carefully. It is difficult to change, even in the middle of customization.

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

Register daemon with WLM DNS
If you use the WLM DNS (connection optimization), you must select this option to register your location service daemon with it. Otherwise, do not select it.

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

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

Generate certificate authority (CA) certificate
Select this option to generate a new CA certificate. Deselect this option to have an existing CA certificate generate server certificates.

Expiration date for certificates
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 did not select the option to generate a certificate authority (CA) certificate.

Note: The date must be specified in YYYY/MM/DD format.

Default SAF keyring name
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
Select this option if you want to enable writable SAF key ring support

Enable SSL on location service daemon
Select this option if you want to support secure communications using Inter-ORB Request Protocol (IIOP) to the location service daemon using SSL. If you do not select this option, a RACF key ring will be generated for the location service daemon to use.

Administrative Security Selection

Use a z/OS security product
Use the z/OS system's SAF-compliant security database to define WebSphere Application Server users

- The SAF security database will be used as the WebSphere Application Server user registry.
- SAF EJBROLE profiles will be used to control role-based authorization, including administrative authority.
- Digital certificates will be stored in the SAF security database.

Choose this option if you plan to use the SAF security database as your WebSphere Application Server user registry or if you plan to set up an LDAP or custom user registry whose identities will be mapped to SAF user IDs for authorization checking.

Use WebSphere Application Server
Use built-in facilities of WebSphere Application Server to manage users, groups, and authorization policy

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

Choose this option if you plan to use an LDAP or custom user registry without mapping of identities to SAF user IDs. The simple file-based user registry is not recommended for production use.

Do not enable security
Do not configure or enable administrative security.

This option is not recommended because it allows anyone to make changes to the WebSphere Application Server configuration.

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

Security Managed by the z/OS Product

SAF profile prefix (optional)
SAF profile prefix

To distinguish between APPL or EJBROLE profiles based on SAF profile prefix, provide an alphanumeric SAF profile prefix of one to eight characters.

All servers in the cell will prepend the SAF profile prefix that you specify to the application-specific J2EE role name to create the SAF EJBROLE profile for checking.

Note: The SAF profile prefix is not used, however, if role checking is performed using WebSphere Application Server for z/OS bindings.

The SAF profile prefix is also used as the APPL profile name and inserted into the profile name used for CBIND checks. The RACF jobs create and authorize the appropriate RACF profiles for the created nodes and servers.

If you do not want to use a SAF profile prefix, leave this field blank.

WebSphere Application Server unauthenticated user

User ID
User ID associated with unauthenticated client requests

This user ID is sometimes referred to as the ″guest″ user ID. It should be given the RESTRICTED attribute in RACF to prevent it from inheriting UACC-based access privileges.

Allow OS security to assign UID
Select this option to have RACF assign an unused UID value.

Allow user-specified UID
Select this option to specify a specific UID value.

UID UNIX System Services UID number for the user ID that will be associated with unauthenticated client requests

Note: UID values must be unique numeric values between 1 and 2,147,483,647.

Security Managed by the WebSphere Family Product

Specify a user name and password to login to the administrative console and perform administrative tasks.

User name
User name for the administrator

Password
Password for the administrator

Note: This password must not be blank.

Security Certificate

Default personal certificate

Issued to distinguished name
Identifier of the personal certificate

It can be customized if necessary. The default syntax for the distinguished name is:

```
cn=<host>,ou=<cell>,ou=<node>,o=<company>,c=<country>
```

Issued by distinguished name
Identifier of the root signing certificate

It can be customized if necessary. The default syntax for the distinguished name is

```
cn=<host>,ou=Root Certificate,ou=<cell>,ou=<node>,
o=<company>,c=<country>
```

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

Root signing certificate

Expiration period in years
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
Default password for all key stores

It should be changed to protect the security of the keystore files and SSL configuration.

Double-byte characters as well as certain ASCII characters such as the asterisk (*) and ampersand (&) are invalid characters for the keystore password.

Job Statement Definition

All the customization jobs that will be tailored for you will need a job statement. Enter a valid job statement for your installation. The customization process will update the job name for you in all the generated jobs, so you need not be concerned with that portion of the job statement. If continuation lines are needed, replace the comment lines with continuation lines.

Job statement 1

Job statement 2

Job statement 3

Job statement 4

Customization worksheet: Secure proxy administrative agent

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 administrative agent:

_____

System name: _____ Sysplex name: _____

Customization Definition Name

Item	Default	Your value
Customization definition name	ZAdminAgent*xx*	
Response file path name (optional)	None	

Default 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	9510	
		Highest default port number	9519	

Target Datasets

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

Configure Common Groups

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

Configure Common Users

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

System and Dataset Names

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

Cell, Node, and Server Names

Item		Default	Your value
Cell names			
	Short name	BBOADMA	
	Long name	bboadma	
Node names			
	Short name	BBOADMA	
	Long name	bboadma	
Server names			
	Short name	BBOADMA	
	Long name	adminagent	adminagent
Cluster transition name		BBOPRXA	

Configuration File System

Item			Default	Your value
Mount point			/wasv7config/*cell_long_name*/*node_long_name*	
Directory path name relative to mount point			SecureProxyAdmin	
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	
* If you select the zSeries File System, you might want to change the extension of this file to .ZFS.				

WebSphere Application Server Product File System

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	

Process Definitions

Item		Default	Your value
Controller process			
	Job name	*server_short_name*	*server_short_name*
	Procedure name	BBO7YCR	
Servant process			
	Job name	*server_short_name*S	*server_short_name*S
	Procedure name	BBO7YSR	

Port Values Assignment

Item	Default	Your value
Node host name or IP address	None	

Item	Default	Your value
JMX SOAP connector port	8880	
Bootstrap port	9807	
Administrative interprocess communication port (K)	9630	

Location Service Daemon Definitions

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	BBODMNY	
Procedure name	BBODMNY	
IP name	*host_name*	
Listen IP	*	
Port	5755	
SSL port	5756	
Register daemon with WLM DNS	Not selected	

SSL Customization

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 writable SAF keyring support	Not selected	
Enable SSL on location service daemon	Selected	

Administrative Security Selection

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

Security Managed by the z/OS Product

Item			Default	Your value
SAF profile prefix			None	
WebSphere Application Server unauthenticated user				
	User ID		WSGUEST	
	Allow OS security to assign UID		Not selected	
	Allow user-specified UID		Selected	
		UID	2402	

Security Managed by the WebSphere Family Product

Item	Default	Your value
User name	WSADMIN	
Password	None	

Security Certificate

Item		Default	Your value
Default personal certificate			
	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			

Job Statement Definition

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

Planning for recovery

About this task

This article helps you plan for any recovery measures that you might need to take.

1. Decide whether or not to implement automatic restart. See “Automatic restart management” on page 278 for more information.
2. Review the recommendations for starting a deployment manager on a different MVS image. See “Starting a deployment manager on a different MVS image” for more information.

Starting a deployment manager on a different MVS image

This describes steps you must follow to start your deployment manager on an MVS image different from the one on which it was originally configured.

About this task

The ability to start your deployment manager on an MVS image different from the one on which it was originally configured is handy if your original system becomes unavailable, either through a planned outage or a system failure. This way, you can still start and stop applications, make configuration updates, utilize monitors that use the PMI interface, perform other control functions, and so on. Perform the following steps to start your deployment manager on a different MVS image and ensure that client requests will successfully find the deployment manager at its new location.

Note: This works only if the deployment manager on the original MVS image is down. WebSphere Application Server for z/OS allows only one copy of the deployment manager to run at one time for any given cell.

1. Ensure that the MVS image to which you are moving the deployment manager contains a node that is already part of the cell of the deployment manager you want to move.
2. Ensure that the location service daemon on the MVS image to which you are moving the deployment manager is up and running before you move the deployment manager.
3. Using the Profile Management Tool or zpmt command, set your host names and ports appropriately:
   - Ensure that the host names and ports for the deployment manager are not specific to a particular system.
   - Ensure that you use a DVIPA generic host name, rather than a system-specific host name, for the node host name and an asterisk (″*″) for both the ORB listener IP address and HTTP transport IP address.
   - Consider configuring a secondary DVIPA in case the system with the primary VIPA is down.
4. Ensure that Sysplex Distributor is enabled so that, regardless of where the DVIPA has moved, it automatically routes any inbound traffic to the deployment manager.
5. Ensure that access to the PROCLIB is the same for both the original MVS image and the MVS image to which you want to move the deployment manager.
6. Start the deployment manager on the new system.

   There are three ways to accomplish this, depending on the configuration of your HFSs. Follow the scenario that matches your configuration.

   Scenario 1: Root HFS is shared among all processors, deployment manager’s configuration is in a configuration HFS on a system-generic mount point.

   Issue the start command for the deployment manager on the system on which you want it to reside:

   - To start the server in 31-bit mode:

     ```
     S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortname>.<node_shortname>.<server_shortname>
     ```

   - To start the server in 64-bit mode:

     ```
     S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortname>.<node_shortname>.<server_shortname>,AMODE=64
     ```

   Scenario 2: Root HFS is shared among all processors, deployment manager’s configuration HFS is mounted under a system-specific directory.

Note: This is an undesirable scenario that you should try to avoid from the start of your system configuration. If you find yourself with this setup, however, follow these steps for the workaround.

a. Create a symbolic link at the equivalent system-specific location on the target MVS image. The contents of the symbolic link should point back to the actual mount point, which means you should not use $SYSNAME anywhere.

b. Issue the start command for the deployment manager on the system on which you want it to reside:

   - To start the server in 31-bit mode:

     ```
     S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortname>.<node_shortname>.<server_shortname>
     ```

   - To start the server in 64-bit mode:

     ```
     S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortname>.<node_shortname>.<server_shortname>,AMODE=64
     ```

Scenario 3: Root HFS is not shared among any processors, deployment manager's configuration HFS is mounted and accessible to only one system at a time.

a. Unmount the configuration HFS from the original MVS image and remount it (at a mount point with the same name) on the new MVS image.

b. Issue the start command for the deployment manager on the system on which you want it to reside:

   - To start the server in 31-bit mode:

     ```
     S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortname>.<node_shortname>.<server_shortname>
     ```

   - To start the server in 64-bit mode:

     ```
     S <controller_procname>,JOBNAME=<jobname>, ENV=<cell_shortname>.<node_shortname>.<server_shortname>,AMODE=64
     ```

Results

You know you are done when your deployment manager is up and running on a different MVS image and you are able to use it to make configuration updates to your environment.

Automatic restart management

WebSphere Application Server for z/OS uses the z/OS automatic restart management (ARM) to recover application servers. Each application server running on a z/OS system (including servers you create for your business applications) are automatically registered with an ARM group. Each registration uses a special element type called SYSCB, which ARM treats as restart level 3, assuring that RRS restarts before any application server.

If you have an application that is critical for your business, you need facilities to manage failures. z/OS provides rich automation interfaces, such as ARM, that you can use to detect and recover from failures. ARM handles the restarting of servers when failures occur.

Note:

- If you have ARM enabled on your system, you might want to disable ARM for the WebSphere Application Server for z/OS address spaces before you install and customize WebSphere Application Server for z/OS. During configuration, job errors might cause unnecessary restarts of the WebSphere Application Server for z/OS address spaces. After installation and configuration, consider enabling ARM.
- If you are ARM-enabled and you cancel or stop a server, it will restart in place using the armrestart command.
- It is a good idea to set up an ARM policy for your deployment manager and node agents.
- If you start the location service daemon on a system that already has one, it will terminate.
- Every other server will come up on a dynamic port unless the configuration has a fixed port. Therefore, the fixed ports must be unique in a sysplex.

- If you issue STOP, CANCEL, or MODIFY commands against server instances, be aware of how automatic restart management behaves regarding WebSphere Application Server for z/OS server instances:

Table 4. Behavior of automatic restart management regarding WebSphere Application Server for z/OS server instances

If you issue . . .	ARM will . . .
STOP *address_space*	not restart the address space
CANCEL *address_space*	not restart the address space
CANCEL *address_space*, ARMRESTART	restart the address space
MODIFY *address_space*, CANCEL	not restart the address space
MODIFY *address_space*, CANCEL,ARMRESTART	restart the address space

Activating automatic restart management

Before you begin

You must have access to the couple dataset format utility, IXCL1DSU, in SYS1.MIGLIB. If you plan to modify the automatic restart management policy, you must have access to the administrative data utility, IXCMIAPU, also in SYS1.MIGLIB, and have UPDATE authorization to the RACF FACILITY class MVSADMIN.XCF.ARM. To start a policy, you must have READ authorization to the RACF FACILITY class MVSADMIN.XCF.ARM.

About this task

Though servers automatically register with automatic restart management, you must activate the arm component itself, which means you must:

1. Allocate an ARM couple dataset.
2. Start the automatic restart management policy.

If automatic restart management is not active, WebSphere Application Server for z/OS issues an error message to the hardcopy log.

You are not required to change the automatic restart management policy. However, you will have to modify this policy if you want to create custom restart groups. For instance, it is not required or recommended that you start the node agent or deployment manager servers on another system. These servers will never have any transactional recovery to perform. Therefore, they should only be set up for restart-in-place. For complete information about how to modify the policies, see *z/OS MVS Setting Up a Sysplex* (SA22-7625).

The following procedure is intended to give you enough information to get automatic restart management running. Defining automatic restart management policies would require the z/OS manual mentioned above.

1. If you have not already formatted a couple dataset for policies, do so now. For details, see *z/OS MVS Setting Up a Sysplex*
2. Submit the job to format the ARM couple dataset.
3. Optional: Modify the automatic restart management policy. To get started, you do not need to modify the policy. If you do want to modify the automatic restart management policy, go to *z/OS MVS Setting Up a Sysplex*, and follow the instructions in that manual.
4. Issue the following operator commands to start the automatic restart management policy:

   ```
   SETXCF COUPLE,TYPE=ARM,PCOUPLE=(dsname,vvvvvv)
   SETXCF START,POLICY,TYPE=ARM
   ```

   where

dsname
Is the dataset name for the couple dataset.

vvvvvv
Is the volume serial of the volume on which the couple dataset resides.

Results

You are done when the SETXCF commands complete successfully.

Displaying the status of ARM-registered address spaces:

WebSphere Application Server for the z/OS operating system ships with all control regions issuing Automatic Restart Management (ARM) registration commands. If your installation enables ARM, you can use ARM to display the status of all ARM-registered address spaces, including the address spaces of server instances.

About this task

ARM is used to restart all address spaces that are registered with ARM if they go down. Address spaces that are canceled are not restarted even if they are registered.

Each WebSphere Application Server for z/OS controller registers with ARM. If a controller terminates abnormally or the system fails, ARM will try to restart the failing address spaces. In doing this, ARM will ensure that dependent address spaces are grouped together and will start in the appropriate order. In general, the default ARM policy will restart WebSphere Application Server for z/OS in place. If you are using a sysplex, see "Automatic restart management" on page 278 for setup guidelines to ensure that no cross-system restarts are performed.

Perform the following steps to use ARM to display the status of ARM registered address spaces (including the address spaces of server instances:

1. Initialize all servers.
2. Display all registered address spaces (including the address spaces of server instances). Issue the following command:

```
d xcf,armstatus,detail
```

Guidelines for changing automatic restart management policies

Because server instances register with the default restart group, automatic restart management (ARM) attempts to restart the entire default group on another system in the sysplex when a system failure occurs. To create a restart group other than this default group, you need to follow certain rules.

If you want to create a restart group other than this default group, you need to comply with the following rules and restrictions that apply for z/OS ARM policies. For more information about how to actually change these policies, see, *z/OS MVS Setting Up a Sysplex* (SA22-7625).

- To change the policy, you need to know the existing element names for the server instances and how to name new elements for additional instances. The element names for these server instances are formed by concatenating the cell short name and the servers specific short name.

  If you have a cell named PLEX1 and server named BBOS001, for example, the ARM element name would be PLEX1BBOS001.

  Since wildcard characters can be used in the ARM policy, it is possible to exclude an entire group of servers by using a common naming scheme within your cell.

  The following section of the ARM policy will prevent any node agents from starting, for example, assuming that each node agent in your cell has a name that adheres to the form BBON*xxx*:

```
RESTART_GROUP(WEBSPHERE)
ELEMENT(PLEX1BBON*)
RESTART_ATTEMPTS(0,150)
RESTART_TIMEOUT(600)
READY_TIMEOUT(1200)
TERMTYPE(ALLTERM)
RESTART_METHOD(BOTH,PERSIST)
```

This ARM policy will also prevent the node agent from restarting in place. This specification can be modified by changing the RESTART_METHOD and TERMTYPE parameters. *See z/OS MVS Setting Up a Sysplex* (SA22-7625) for more information.

- If you create a restart group, keep the following in the same restart group and set the restart order for the elements as indicated:
  1. RRS
  2. DB2 with IRLM, IMS, CICS, and other transaction or resource managers if used by your application servers in the restart group
  3. Your server instances

Either set up the location service daemon and node agent for restart-in-place or remove them from your ARM policy. Since WebSphere Application Server must be running on all systems that might be used to perform recovery, the application servers will use the location service daemon and node agent that are already running on the alternate system. If the location service daemon attempts to restart on the alternate system, it will fail. If the node agent restarts on the alternate system, it will have no recovery work to do.

Displaying the status of ARM-registered address spaces

WebSphere Application Server for the z/OS operating system ships with all control regions issuing Automatic Restart Management (ARM) registration commands. If your installation enables ARM, you can use ARM to display the status of all ARM-registered address spaces, including the address spaces of server instances.

About this task

ARM is used to restart all address spaces that are registered with ARM if they go down. Address spaces that are canceled are not restarted even if they are registered.

Each WebSphere Application Server for z/OS controller registers with ARM. If a controller terminates abnormally or the system fails, ARM will try to restart the failing address spaces. In doing this, ARM will ensure that dependent address spaces are grouped together and will start in the appropriate order. In general, the default ARM policy will restart WebSphere Application Server for z/OS in place. If you are using a sysplex, see “Automatic restart management” on page 278 for setup guidelines to ensure that no cross-system restarts are performed.

Perform the following steps to use ARM to display the status of ARM registered address spaces (including the address spaces of server instances:

1. Initialize all servers.
2. Display all registered address spaces (including the address spaces of server instances). Issue the following command:

   ```
   d xcf,armstatus,detail
   ```

Problem diagnostic plan strategy

Use component trace (CTRACE) to capture and display trace data in trace datasets. Use error log stream to review records that contain error information when WebSphere Application Server for z/OS detects an unexpected condition or failure within its own code. Use BBORBLOG to browse the error log stream.

You can use the following diagnostic tools:

- Component trace
- Error log stream
- Dump datasets

Overview of problem diagnosis

WebSphere Application Server for z/OS uses component trace (CTRACE) to capture and display trace data in trace datasets. WebSphere Application Server for z/OS identifies itself to CTRACE with the short cell name. CTRACE allows you to perform the following tasks:

- Merge multiple traces through the browse tool, including other components such as TCP/IP and z/OS UNIX.
- Write trace data to a dataset rather than to STDOUT, keeping spool space free.
- Better manage system resources by allowing trace data to wrap or not wrap.
- Use CTRACE to funnel trace data from multiple address spaces to one data set, or have CTRACE send the trace data from each address space to separate datasets.
- Start and stop tracing without stopping and restarting WebSphere Application Server for z/OS address spaces.
- Use one or more datasets for capturing trace data, thus allowing you to manage I/O more effectively.

WebSphere Application Server for z/OS also has an error log stream that records the following error information when WebSphere Application Server for z/OS detects an unexpected condition or failure within its own code:

- Assertion failures
- Unrecoverable error conditions
- Vital resource failures, such as memory
- Operating system exceptions
- Programming defects in WebSphere Application Server for z/OS code

Use the error log stream in conjunction with other facilities available to capture error or status information—such as an activity log, trace data, system logrec, and job log.

The WebSphere Application Server for z/OS error log stream is a system logger application. Because the error log stream uses the system logger, you can perform the following tasks:

- Have error information written to a coupling facility log stream, which provides sysplex-wide error logging, or to a DASD-only log stream, which provides single system-only error logging.

  Note: There is a significant performance penalty when using DASD-only error logging.
- Set up either a common log stream for all of WebSphere Application Server for z/OS or individual log streams servers.

  Local z/OS client ORBs can also log data in log streams. Because the system logger APIs are unauthorized, any application can use them. You should control access to the log streams through a security product such as RACF.

WebSphere Application Server for z/OS provides a REXX™ EXEC (BBORBLOG) that allows you to browse the error log stream. By default, the EXEC formats the error records to fit a 3270 display.

Information about using the error log stream to diagnose problems is in the Troubleshooting section of the WebSphere Application Server information center. General information and guidance about the system logger is in *z/OS MVS Setting Up a Sysplex*.

Table 5. Finding WebSphere Application Server for z/OS Error Log Stream Information

What is your goal?	You should read:
Learn about the system logger and understand its requirements	*z/OS MVS Setting Up a Sysplex*
Learn about the WebSphere Application Server for z/OS error log stream	This article
Size the coupling facility structure space needed for the WebSphere Application Server for z/OS error log stream	*z/OS MVS Setting Up a Sysplex*
Define the WebSphere Application Server for z/OS error log stream	
View the WebSphere Application Server for z/OS error log stream	The Troubleshooting section of the WebSphere Application Server information center
Learn about how Java applications can log messages and trace data in the error log stream	The Applications section of the WebSphere Application Server information center

For details about problem diagnosis, see the Troubleshooting section of the WebSphere Application Server information center.

Planning for component trace

To use CTRACE, perform the following tasks:

- Specify trace options for identifying trace datasets and connecting WebSphere Application Server for z/OS address spaces to the datasets in parmlib members.
- Update WebSphere Application Server for z/OS WebSphere variables to allow for initial trace parameters.
- Use IPCS-CTRACE to view the trace data because you cannot read the trace data in an ordinary editor.

Recommendation for dumps

Plan as you would normally for system dumps. Due to the size of WebSphere Application Server for z/OS address spaces, you might need to resize your system dump datasets and use dynamic dump datasets.

Chapter 9. Configuring the WebSphere Application Server for z/OS product after installation

Use this task to configure WebSphere Application Server for z/OS application serving environments for your z/OS target systems.

Before you begin

- Select a z/OS target system and complete the steps in Chapter 6, “Installing the product and additional software,” on page 35 and Chapter 7, “Preparing the base operating system,” on page 39.
- Choose a WebSphere Application Server for z/OS configuration (practice, standalone, or Network Deployment cell) and complete the steps in Chapter 8, “Planning for product configuration,” on page 49.

About this task

Configuring a WebSphere Application Server for z/OS application serving environment consists of:

1. Setting up the WebSphere Application Server for z/OS configuration directory for the environment
2. Making any required changes to the z/OS target system that pertain to the particular application serving environment
3. Starting the new environment to verify the configuration

Configuring these application serving environments after product installation requires a fair amount of planning and coordination. If you have not previously configured WebSphere Application Server for z/OS, you should configure a ″practice″ standalone application server using the default options then proceed to configure the actual product configuration that you want. See “Building a practice WebSphere Application Server for z/OS cell” on page 84 for more information.

WebSphere Application Server for z/OS application serving environment nodes can be created using the workstation-based Profile Management Tool (see “Configuring z/OS application-serving environments with the Profile Management Tool”) or the zpmt command.

Once a node is configured and running, make further changes using the Web-based administrative console or scripting.

What to do next

Once your application serving environment is up and running, you can install and test applications.

Configuring z/OS application-serving environments with the Profile Management Tool

You can configure z/OS application serving environments for your z/OS target systems using the Profile Management Tool.

Before you begin

- Choose a z/OS target system, and complete the steps for installing the product and additional software and preparing the base operating system.
- Check that an FTP server is running on the z/OS target system.
- Choose the type of application server environment that you want to configure, and complete the planning steps for that configuration.

About this task

Note: 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 profiles and upload the associated jobs and instructions to the target z/OS system.

Configuring a z/OS system application serving environment consists of setting up the application server z/OS environment configuration directory, making required changes to the z/OS target system that pertain to the particular application serving environment, and starting the new environment to verify the configuration. Configuring these application serving environments after product installation requires planning and coordination. If you have not previously configured the application server for z/OS systems, you need to configure a practice standalone application server using the default options. The next step is to configure the product configuration that you want. Read about using the Profile Management Tool, building a practice application server for a z/OS cell and considerations about WebSphere Application Server for z/OS maintenance for more information.

If you have already created a Network Deployment cell, follow the instructions in this topic to expand the cell by creating a new federated node or federating an existing standalone application server node into the Network Deployment cell.

WebSphere Application Server for z/OS application serving environment nodes are created using batch jobs that are build 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 z/OS operating system, prepared your z/OS target systems, and planned your new application server environment, perform these tasks to configure and start the application server environment.

1. Review the procedures in “Using the Profile Management Tool” on page 287.
2. Install WebSphere Customization Tools Version 7.0.
   Read “Installing and updating Websphere Customization Tools” on page 37 for more information.
3. Choose the task for the type of application server environment that you want to configure from the following tasks:
   - “Creating a standalone application server cell” on page 291
   - “Creating a deployment manager” on page 292
   - “Creating a Network Deployment cell with an application server” on page 298
   - “Creating a managed node” on page 295
   - “Federating a standalone application server into a Network Deployment cell” on page 297
   - “Creating an administrative agent” on page 292
   - “Creating a job manager” on page 299
   - “Creating a secure proxy administrative agent” on page 300
   - “Creating a secure proxy server” on page 299

What to do next

After your application serving environment is running, you can install and test your applications. You might also want to configure your Web servers to interact with your z/OS system.

Note: If you configured WebSphere Application Server for z/OS using the English Profile Management Tool and want to allow the display of Japanese characters correctly in your environment, you need to modify some script files.

1. Edit the setupCmdLine.sh file
   from: CONSOLE_ENCODING=″-Dws.input.encoding=cp1047 -Dws.output.encoding=cp1047″

to: CONSOLE_ENCODING=″-Dws.input.encoding=cp1399 -Dws.output.encoding=cp1399″

2. Edit the wsadmin.sh file

   from: EXTRA_D_ARGS=″-Dfile.encoding=ISO8859-1

   to: EXTRA_D_ARGS=″-Dfile.encoding=IBM-932

Making these two changes will enable you to see the Japanese messages correctly.

Using the Profile Management Tool

The Profile Management Tool is a tool, running under the WebSphere Customization Tools, that you use for the initial setup of WebSphere Application Server for z/OS Version 7.0 cells and nodes.

Before you begin

Install the most current release of WebSphere Customization Tools Version 7.0 on a workstation running the Windows or Linux Intel operating system. Read “Installing and updating Websphere Customization Tools” on page 37 for more information.

About this task

The Profile Management Tool itself does not create the cells and nodes; instead, it creates batch jobs, scripts, and data files that you can use to perform WebSphere Application Server for z/OS customization tasks. These jobs, scripts, and data files form a customization definition on your workstation that is then uploaded to z/OS and used for customization.

Note:

- Do not use the z/OS Profile Management Tool for WebSphere Application Server Version 6.1, which runs under the Application Server Toolkit, to set up Version 7.0 cells and nodes.
- In WebSphere Application Server for z/OS, you use the Profile Management Tool and the jobs that it generates to create new cells and nodes. After you have created a standalone application server or Network Deployment cell, however, you use the WebSphere Application Server for z/OS administrative console or scripting to administer it.

The Profile Management Tool is intended for use by a systems programmer or WebSphere Application Server for z/OS administrator who is familiar with the z/OS target system on which the resulting WebSphere Application Server for z/OS cells and nodes will run.

The Profile Management Tool uses response files to hold the various values used to create WebSphere Application Server for z/OS customization jobs, scripts and files. These response files remain on the workstation where the Profile Management Tool is run.

- The Profile Management Tool allows you to put these response files on network drives where they can be shared with other users.
- The Profile Management Tool also uploads the associated response file to a DATA member as part of the upload process. This DATA PDS member can then be downloaded to serve as a basis for a new configuration.

1. Start the Profile Management Tool.

   Read “Starting the Profile Management Tool” on page 288 for more information.
2. Create your customization definitions.

   Read “Creating the customization definition” on page 288 for more information.
3. Optional: Modify the variables in your customization definitions.
4. Optional: Delete any existing customization definitions that you want to remove.
   a. In the WebSphere Application Server for z/OS customization definition table, select the customization definition that you want to delete.

b. Click **Delete**.
c. Click **Yes**.

5. Optional: Review your customization definitions.
   Read “Reviewing the customization definition” on page 290 for more information.
6. Upload your customization jobs to a target z/OS system, or export the jobs to the local file system.
   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.

Starting the Profile Management Tool

This article leads you through the tasks involved in starting and using the Profile Management Tool.

Before you begin

Install the most current release of WebSphere Customization Tools Version 7.0 on a workstation running the Windows or Linux Intel operating system. Read “Installing and updating Websphere Customization Tools” on page 37 for more information.

1. Go to **Start > Programs > IBM WebSphere > WebSphere Customization Tools V7.0** , and click **WebSphere Customization Tools**.
2. If the Profile Management Tool (z/OS only) is not already open, perform the following actions:
   a. Open the **Welcome** tab, and select **Profile Management Tool (z/OS only)**.
   b. Read the Welcome information, and then click **Launch Selected Tool**.

What to do next

You can now create or work with a WebSphere Application Server for z/OS Version 7.0 customization definition.

Creating the customization definition

This article leads you through the tasks involved in creating the customization profile.

Before you begin

Print and complete one of the following worksheets for a customization definition:

Version 7.0	**Version 6.1**
“Customization worksheet: Standalone application server for Version 7.0” on page 101	“Customization worksheet: Standalone application server for Version 6.1” on page 108
“Customization worksheet: Deployment manager for Version 7.0” on page 145	“Customization worksheet: Deployment manager for Version 6.1” on page 151
“Customization worksheet: Managed (custom) node for Version 7.0” on page 168	“Customization worksheet: Managed (custom) node for Version 6.1” on page 174
“Customization worksheet: Federating an application server for Version 7.0” on page 184	“Customization worksheet: Federating an application server for Version 6.1” on page 187
“Customization worksheet: Network Deployment cell with an application server for Version 7.0” on page 207	“Customization worksheet: Network Deployment cell with an application server for Version 6.1” on page 216
“Customization worksheet: Job manager” on page 237	
“Customization worksheet: Administrative agent” on page 127	
“Customization worksheet: Secure proxy server” on page 254	

Version 7.0	Version 6.1
"Customization worksheet: Secure proxy administrative agent" on page 271	

Note:

- The worksheets in the first column of this table are only applicable to creating Version 7.0 customization definitions.
- The worksheets contained in the information center for WebSphere Application Server Version 6.1.x cannot be used for creating Version 6.1 customization definitions using the Profile Management Tool that is part of WebSphere Customization Tools Version 7.0.

About this task

A customization definition consists of a set of files on your workstation that is uploaded to z/OS and used to perform customization tasks.

Use the completed worksheet as a reference when you create your customization definition.

1. Start the Profile Management Tool.

   Read "Starting the Profile Management Tool" on page 288 for more information.
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.

      Note: 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 a version.
   d. Click **Finish**.
3. In the **Customization Locations** table, select the location of the customization definition that you want to create.
4. Click the **Customization Definitions** tab if it is not already selected.
5. Click **Create**.
6. 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.

   Note:
   - Hover your cursor over a field for help information.
   - You can also refer to the definitions of the Version 7.0 variables in the following articles:
     – "Customization variables: Standalone application server cell" on page 86
     – "Customization variables: Deployment manager" on page 133
     – "Customization variables: Managed (custom) node" on page 157
     – "Customization variables: Federating an application server" on page 180

- "Customization variables: Network Deployment cell with an application server" on page 189
- "Customization variables: Job manager" on page 225
- "Customization variables: Administrative agent" on page 115
- "Customization variables: Secure proxy server" on page 243
- "Customization variables: Secure proxy administrative agent" on page 260

- 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.

7. Click **Finish**.

Note:

- 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.

Reviewing the customization definition

This article explains how to work with a customization definition that you have created in the Profile Management Tool.

1. Start the Profile Management Tool.

   Read "Starting the Profile Management Tool" on page 288 for more information.
2. In the **Customization Locations** table, select the location of the customization definition that you want to review.
3. In the **Customization Definitions** table, select the customization definition that you want to review.
4. Click the appropriate tabs for information about the customization definition.
   - Click the **Customization Summary** tab for general information about the customization definition.
   - Click the **Customization Instructions** tab for a copy of the customized instructions that were generated when the customization definition was created.

     These are the instructions that you use to perform the actual customization after you upload the customization definition to the z/OS target system.
   - Click the **Customization Response File** tab for a copy of the response file that was generated when the customization definition was created.

Processing customization definitions using the Profile Management Tool

You can upload the jobs associated with a z/OS customization definition to partitioned data sets on a target z/OS system or export them to a directory on the workstation where the Profile Management Tool is running.

Before you begin

Create the customization definition for the jobs that you want to upload to a target z/OS system or export to the local file system. Read "Creating the customization definition" on page 288 for more information.

1. Start the Profile Management Tool.

   Read "Starting the Profile Management Tool" on page 288 for more information.
2. In the **Customization Locations** table, select the location of the customization definition that you want to process.
3. In the **Customization Definitions** table, select the customization definition that you want to process.

4. Click **Process**.
5. On the **Select Process Type** panel, select the type of processing that you want to perform on the customization definition.
6. Click **Next**.
7. Depending on the type of process that you selected, perform one of the following actions:
   - On the **Upload Customization Definition** panel, specify the necessary upload information.
     a. In the **Target z/OS system** field, enter the IP name or address of the z/OS system to which you want to upload the customization jobs.
     b. In the **User ID** field, enter the user ID that you want to use to log on to the FTP server on the target z/OS system.
     c. In the **Password** field, enter the password for the user ID that you want to use to log on to the FTP server on the target z/OS system.
     d. In the **Server port** field, enter the port number of the FTP server on the target z/OS system.
     e. In the **Timeout** field, enter the number of seconds that can elapse without any I/O operation completing before the upload is stopped.
     f. If you want to allocate the target z/OS datasets, check the box beside **Allocate target z/OS datasets** and complete the two fields that are activated.

        Note: If you are uploading the customization jobs to a system different from the system on which you want to run the jobs, you must target a volume that is shared by those systems.

        1) In the **Volume** field, enter the volume for the target datasets.
        2) In the **Unit** field, enter the unit for the target datasets.
   - On the **Export Customization Definition** panel, specify the directory to which you want to export the customization jobs.

     Note: You should not specify an alternate path for the export directories if you might later want to edit any of the generated jobs and then use the upload function to upload the updated jobs to the target z/OS operating system. If you specify an alternate directory, it will be up to you to get the batch jobs to the target z/OS operating system.

   Note:
   - Hover your cursor over a field for help information.
   - Click **Cancel** to leave without processing the customization jobs.
8. Click **Finish**.

Creating a standalone application server cell

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS standalone application server environment using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for a standalone application server cell” on page 86 and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the standalone application server.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Application server** under **WebSphere Application Server for z/OS** for the environment.
   c. Complete the fields using the values from your “Customization worksheet: Standalone application server for Version 7.0” on page 101 as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.

   Read “Reviewing the customization definition” on page 290 for more information.

3. Upload the customization jobs to the target z/OS system.

   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOSSINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new standalone application server should be running on the z/OS system.

You can now deploy and test applications on your new standalone application server.

Creating an administrative agent

You can set up a WebSphere Application Server for z/OS administrative agent using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning for an administrative agent and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the administrative agent.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Management** under **WebSphere Application Server for z/OS** for the environment.
   c. Complete the fields using the values from your completed “Customization worksheet: Administrative agent” on page 127 as you proceed through the panels.

      Select **Administrative agent** for the server type.
2. Review the customization definition to make sure that all of the values are correct.

   Read “Reviewing the customization definition” on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.

   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new administrative agent should be running on the z/OS operating system.

What to do next

Register or deregister nodes using the following methods:

- Register a node by issuing the registerNode command.
- Deregister a node by issuing the deregisterNode command.

Creating a deployment manager

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS Network Deployment cell using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for a Network Deployment cell” on page 133 and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the deployment manager.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Management** under **WebSphere Application Server for z/OS** for the environment.
   c. Complete the fields using the values from your “Customization worksheet: Deployment manager for Version 7.0” on page 145 as you proceed through the panels.

      Select **Deployment manager** for the server type.
2. Review the customization definition to make sure that all of the values are correct.

   Read “Reviewing the customization definition” on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.

   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new Network Deployment cell should be running on the z/OS system. Read “Working with your new deployment manager” for more information.

What to do next

Add application server nodes to your cell using one of two methods:

- Create a new managed node using the Profile Management Tool, and add application servers to it using the administrative console or scripting.
- Federate existing standalone application servers into your Network Deployment cell to create federated nodes with application servers.

Working with your new deployment manager

Once you complete the customization instructions, you will have a WebSphere Application Server for z/OS Network Deployment cell. The Network Deployment cell consists of a deployment manager and a location service daemon. (To run Java EE applications, you must add application server nodes. See below for details.) This article provides useful information for working with your new Network Deployment cell.

Before you begin

Make sure that the WebSphere Application Server for z/OS product HFS and configuration HFS are mounted.

1. To start your deployment manager, issue the following MVS console command:

   ```
   START server_proc,JOBNAME=dmgr_name,ENV=cell_name.node_name.dmgr_name
   ```

   where:
   - *server_proc* is the deployment manager controller cataloged procedure.
   - *dmgr_name* is the deployment manager short name.
   - *node_name* is the deployment manager node short name.
   - *cell_name* is the cell short name.

If you chose default values, for example, you would enter the following START command:

```
START BBO7DCR,JOBNAME=BBODMGR,ENV=BBOCELL.BBODMGR.BBODMGR
```

The START command brings up the deployment manager controller. The controller starts the location service daemon, then uses WLM to start the deployment manager servant. You should see a message similar to the following when the deployment manager is up and running:

```
BBOO0019I INITIALIZATION COMPLETE FOR WEBSPHERE FOR Z/OS CONTROL PROCESS BBODMGR
```

2. Once the deployment manager is successfully started, access the administrative console by pointing a Web browser to the following URL:

   ```
   http://hostname:http_port/ibm/console
   ```

   where:

   - *hostname* is the deployment manager HTTP transport host name that you specified during customization.

     Note: If you specified ″*″ for the deployment manager HTTP host name, this is actually the deployment manager node host name.

   - *http_port* is the deployment manager HTTP port that you specified during customization.

     Note: The default HTTP port for the deployment manager is 9060.

   Until global security is enabled, you will see a signon screen that asks you for a user ID.

   The user ID needs to be the one defined during the customization of the dmgr.

   You can use the administrative console, scripting, or both to manage the Network Deployment cell and deploy and manage Java EE applications. Before you can deploy applications, however, you need to add application server nodes to your Network Deployment cell.

3. Add an application server node to a Network Deployment cell using one of two methods:

   - Create an (empty) managed node using the Profile Management Tool or zpmt command. The new node can reside on the same or a different z/OS system as the deployment manager. The new managed node, consisting of just a node agent and perhaps a location service daemon, is federated into the Network Deployment cell. Once this is done, you can use the administrative console or scripting to add application servers and deploy and manage Java EE applications in the node.

     See the section ″Planning for a new managed node in a Network Deployment cell″ in the *Installing your application serving environment* PDF for more information.

   - Federate an existing standalone application server into the Network Deployment cell. The standalone server node becomes a managed node in the Network Deployment cell, along with any Java EE applications that have been deployed on it.

     See the section ″Planning to federate a standalone server into a Network Deployment cell″ in the *Installing your application serving environment* PDF for more information.

   Application server nodes (also called managed nodes) in a Network Deployment cell consist of a node agent and any number of application servers per node.

   Note: Each z/OS system also needs one location service daemon for each standalone or Network Deployment cell hosted on the system.

4. Use one of the following two methods to stop your deployment manager:

   - Stop the location service daemon, which also stops the deployment manager and any of the cell's managed nodes on the same z/OS system. The location service daemon holds pointers to modules in common storage, and stopping it forces the cell's nodes on the same z/OS system as the location service daemon to shut down. To stop the location service daemon, enter the following MVS console command:

     ```
     STOP daemon_jobname
     ```

where *daemon_jobname* is the location service daemon job name. The default location service daemon job name for a Network Deployment cell is BBODMNC.

Note: This is the easiest way to stop the deployment manager.

- Stop just the deployment manager, leaving the location service daemon and any managed nodes on the z/OS system still running. This works because the deployment manager is used to administer only the cell--it does not need to be up for Java EE applications in the cell to run. To stop the deployment manager, enter the following MVS console command:

  `STOP dmgr_name`

  where *dmgr_name* is the deployment manager short name. The default deployment manager short name is BBODMGR.

Creating a managed node

This article leads you through the tasks involved in creating a customization definition for a managed server node using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for a new managed node in a Network Deployment cell” on page 157 and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the managed node.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Managed (custom) node** under **WebSphere Application Server for z/OS** for the environment.
   c. Complete the fields using the values from your “Customization worksheet: Managed (custom) node for Version 7.0” on page 168 as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.

   Read “Reviewing the customization definition” on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.

   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOMNINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new Network Deployment cell should be running on the z/OS system. Read “Working with your new managed server node” for more information.

Working with your new managed server node

Once you complete the customization instructions, you will have a WebSphere Application Server for z/OS application server node (managed node) in your Network Deployment cell.

Before you begin

Make sure that the WebSphere Application Server for z/OS product HFS and configuration HFS are mounted.

1. Start your node agent by issuing the following MVS console command:

   `START server_proc,JOBNAME=nodeagent_name,ENV=cell_name.node_name.nodeagent_name`

where:

- *server_proc* is the node agent cataloged procedure.
- *nodeagent_name* is the node agent short name.
- *node_name* is the node short name.
- *cell_name* is the cell short name.

If you chose default values for example (your sysplex is named CELL1 and your system is named MVSA), you would enter the following START command:

```
START BBO7ACR,JOBNAME=BBON001,ENV=CELL1.MVSA.BBON001
```

The START command brings up the node agent. The node agent starts the location service daemon (if one is not already running). You should see a message like the following when the node is up and running:

```
BBOO0019I INITIALIZATION COMPLETE FOR WEBSPHERE FOR z/OS CONTROL PROCESS BBON001The node agent must be running in order
the node.
```

2. When the deployment manager for the cell is up and running, access the administrative console by pointing a Web browser to the following URL:

   ```
   http://hostname:http_port/ibm/console
   ```

   where:

   - *hostname* is the deployment manager HTTP transport host name that you specified during customization.

     Note: If you specified ″*″ for the deployment manager HTTP host name, this is actually the deployment manager node host name.
   - *http_port* is the deployment manager HTTP port that you specified during customization.

     Note: The default HTTP port for the deployment manager is 9060.

   Until administrative security is enabled, you will see a signon screen that asks you for a user ID but no password.

   The user ID can be anything and is used only to provide basic tracking of changes. Be aware that until you enable administrative security, anyone with a Web browser and access to the HTTP port can modify your application serving environment.

   You can use the administrative console, scripting, or both to manage the node and deploy and manage J2EE applications. Before you can deploy applications, however, you need to add application servers to your managed node.
3. Application servers can be added to the managed server node using the administrative console or scripting. Either of two methods can be used:
   - Create a new application server directly using the administrative console or scripting. You can use the controller, servant and CRA cataloged procedures and user IDs created during the managed node setup process for any application servers you create in the managed node.
   - Cluster an existing application server in another node, using this managed node as a target. This will create a ″cloned″ copy of the application server being clustered in your new managed node.
4. To start one of your managed node's application servers, issue the following MVS console command:

   ```
   START server_proc,JOBNAME=server_name,ENV=cell_name.node_name.server_name
   ```

   where:

   - *server_proc* is the application server agent cataloged procedure (can be the same as the node agent cataloged procedure).
   - *nodeagent_name* is the application server short name.
   - *node_name* is the node short name.

- *cell_name* is the cell short name.

If you chose the default procedure name for example (your sysplex is named CELL1, your node is named MVSA, and your server is named AZSR01A), you would enter the following START command:

```
START BBO7ACR,JOBNAME=AZSR01A,ENV=CELL1.MVSA.AZSR01A
```

The START command brings up the application server controller. The controller starts the location service daemon (if one is not already running) and then uses WLM to start the control region adjunct and the servants. You should see a message similar to the following when the node is up and running:

```
BBOO0019I INITIALIZATION COMPLETE FOR WEBSPHERE FOR Z/OS CONTROL PROCESS AZSR01A
```

5. Use one of the following two methods to stop your deployment manager:
   - Stop the location service daemon, which also stops any of the cell's nodes on the same z/OS system. The location service daemon holds pointers to modules in common storage, and stopping it forces all cell members on the same z/OS system as the daemon to shut down. To stop the location service daemon, enter the following MVS console command:

     ```
     STOP daemon_jobname
     ```

     where *daemon_jobname* is the location service daemon job name. The default location service daemon job name for a Network Deployment cell is BBODMNC.
   - Stop just the node agent and its application servers while leaving the location service daemon, deployment manager (if present), and any other managed nodes on the z/OS system still running. To stop the node agent, enter the following MVS console command:

     ```
     STOP nodeagent_name
     ```

     where *nodeagent_name* is the node agent short name. The default node agent short name is BBON001.

Federating a standalone application server into a Network Deployment cell

This article leads you through the tasks involved in federating a WebSphere Application Server for z/OS standalone application server into a Network Deployment cell using the Profile Management Tool.

1. Create a customization definition for federating the standalone application server into a Network Deployment cell.
   a. Follow the instructions in "Creating the customization definition" on page 288.
   b. Select **Federate an application server** under **WebSphere Application Server for z/OS** for the environment.
   c. Complete the fields using the values from your "Customization worksheet: Federating an application server for Version 7.0" on page 184 as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.

   Read "Reviewing the customization definition" on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.

   Read "Processing customization definitions using the Profile Management Tool" on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOANINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new federated application server should be running on the z/OS system. Read "Working with your new federated server node" on page 298 for more information.

Working with your new federated server node

- Check the default host alias list and all other cell-level documents to see if any need to be added in support of the applications and application servers on the newly federated node. Cell-level documents are not automatically updated by the federation process.
- Remove the location service daemon port definitions from your TCP/IP profile for the standalone application server cell because these are not used after federation.

What to do next

Note that Web server configurations in an unmanaged node in a standalone application server cell are not migrated as part of federation. Use the administrative console or scripting to add new Web Server definitions to a Network Deployment cell.

Once these tasks are accomplished, a federated application server node is just like any other application server node. The primary difference is that it already has an application server and applications if they were federated as well. Read “Working with your new managed server node” on page 295 for further information.

Creating a Network Deployment cell with an application server

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS Network Deployment cell including an initial application server, using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of “Planning for a Network Deployment cell” on page 133 and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the Network Deployment cell.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Cell (deployment manager and an application server)** under **WebSphere Application Server for z/OS** for the environment.
   c. Complete the fields using the values from your “Customization worksheet: Deployment manager for Version 7.0” on page 145 as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.

   Read “Reviewing the customization definition” on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.

   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBODMINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new Network Deployment cell should be running on the z/OS system. Read “Working with your new deployment manager” on page 293 for more information.

What to do next

Add application server nodes to your cell using one of two methods:

- Create a new managed node using the Profile Management Tool, and add application servers to it using the administrative console or scripting.

- Federate existing standalone application servers into your Network Deployment cell to create federated nodes with application servers.

Creating a job manager

You can set up a WebSphere Application Server for z/OS job manager using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning a job manager and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the job manager.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Management** under **WebSphere Application Server for z/OS** for the environment.
   c. Complete the fields using the values from your “Customization worksheet: Job manager” on page 237 as you proceed through the panels.

      Select **Job manager** for the server type.
2. Review the customization definition to make sure that all of the values are correct.

   Read “Reviewing the customization definition” on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.

   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new job manager should be running on the z/OS operating system.

What to do next

To register application server nodes and deployment managers with the job manager, use the wsadmin registerWithJobManager command. The command is in the ManagedNodeAgent command group.

Creating a secure proxy server

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS secure proxy server using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning for a secure proxy server and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the secure proxy server.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Secure proxy** under **WebSphere DMZ Secure Proxy Server** for the environment.
   c. Complete the fields using the values from your “Customization worksheet: Secure proxy server” on page 254 as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.

   Read “Reviewing the customization definition” on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.

Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.

4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOSSINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new secure proxy server should be running on the z/OS system.

Creating a secure proxy administrative agent

This article leads you through the tasks involved in setting up a WebSphere Application Server for z/OS administrative agent using the Profile Management Tool.

Before you begin

Have available copies of the worksheets that you completed as a part of planning for an administrative agent and Chapter 8, “Planning for product configuration,” on page 49.

1. Create a customization definition for the administrative agent.
   a. Follow the instructions in “Creating the customization definition” on page 288.
   b. Select **Management** under **WebSphere DMZ Secure Proxy Server** for the environment.
   c. Complete the fields using the values from your “Customization worksheet: Secure proxy administrative agent” on page 271 as you proceed through the panels.
2. Review the customization definition to make sure that all of the values are correct.
   Read “Reviewing the customization definition” on page 290 for more information.
3. Upload the customization jobs to the target z/OS system.
   Read “Processing customization definitions using the Profile Management Tool” on page 290 for more information.
4. To run the customization jobs on the target z/OS system, follow the instructions in the **Customization Instructions** view of the Profile Management Tool or in the BBOCCINS member of the CNTL dataset that you uploaded.

Results

When you have successfully completed the steps in the generated instructions, the new administrative agent should be running on the z/OS system.

Configuring with symbolic links for z/OS

Symbolic links can be used in configuring and maintenance for WebSphere Application Server for z/OS applications.

About this task

When a WebSphere Application Server for z/OS node is built, the configuration HFS is peppered with hundreds of symbolic links. These symbolic links point to files in the ″product HFS″ supplied by IBM. There is good reason for having this design. Unfortunately, if you configure two or more nodes that point directly to the mount point of the product HFS, then applying maintenance to the product HFS necessarily means updating all the nodes at once.

The way to provide flexibility is to configure what is known as an intermediate symbolic link between the node’s configuration HFS and the actual mount point of the product HFS. The result is two symbolic links:

the configuration HFS link pointing to the intermediate link, and the intermediate link then pointing to the product HFS. The value of this is that a node can ″point″ to a new level of the product HFS by simply changing the one intermediate symbolic link.

What to do next

Read http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100396 for additional information on the use of intermediate symbolic links.

Configuring z/OS application-serving environments with the zpmt command

You can configure WebSphere Application Server for z/OS application-serving environments for your z/OS target systems using the zpmt command. The zpmt command creates the same batch jobs and data files as the workstation-based Profile Management Tool, but the command runs under z/OS rather than on a workstation.

Before you begin

- Choose a z/OS target system and complete the steps in Chapter 6, “Installing the product and additional software,” on page 35 and Chapter 7, “Preparing the base operating system,” on page 39.
- Choose the type of application server environment that you want to configure, and complete the planning steps for that configuration.

About this task

Note: The zpmt command is an alternative to the Profile Management Tool 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.

Configuring a WebSphere Application Server for z/OS application serving environment consists of setting up the WebSphere Application Server for z/OS configuration directory for the environment, making any required changes to the z/OS target system that pertain to the particular application serving environment, and starting the new environment to verify the configuration. Configuring these application serving environments after product installation requires a fair amount of planning and coordination. If you have not previously configured WebSphere Application Server for z/OS, you should configure a ″practice″ standalone application server using the sample response file. Then proceed to configure the actual product configuration that you want. See the sample files below for more information.

WebSphere Application Server for z/OS application serving environment nodes are created using batch jobs that are build 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. 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.
   - For a standalone application server, refer to the list of variables and definitions in “Variables for configuring a standalone application server using the zpmt command” on page 304 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

- For a deployment manager, refer to the list of variables and definitions in "Variables for configuring a deployment manager using the zpmt command" on page 314 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.
- For a managed (custom) node, refer to the list of variables and definitions in "Variables for configuring a managed (custom) node using the zpmt command" on page 323 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.
- For a federated node, refer to the list of variables and definitions in "Variables for federating an application server using the zpmt command" on page 331 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.
- For a Network Deployment cell with an application server, refer to the list of variables and definitions in "Variables for configuring a Network Deployment cell with an application server using the zpmt command" on page 334 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.
- For an administrative agent, refer to the list of variables and definitions in "Variables for configuring an administrative agent using the zpmt command" on page 348 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.
- For a job manager, refer to the list of variables and definitions in "Variables for configuring a job manager using the zpmt command" on page 357 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.
- For a secure proxy server, refer to the list of variables and definitions in "Variables for configuring a secure proxy server using the zpmt command" on page 365 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.
- For a secure proxy administrative agent, refer to the list of variables and definitions in "Variables for configuring a secure proxy administrative agent using the zpmt command" on page 374 and the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

2. On your target z/OS system, run the zpmt.sh shell script using your prepared response file. This tool will create the .CNTL and .DATA files needed to run the required jobs. The response file needs to be located in the UNIX (USS) file system. For command syntax, refer to the zpmt.sh shell script file: "zpmt command."
3. Follow the instructions in the *xxxxx*INS member of the .CNTL data to create the application serving environment.

What to do next

When your application serving environment is running, you can install and test your applications. You might also want to configure your Web servers to interact with WebSphere Application Server for z/OS.

Note: If you configured WebSphere Application Server for z/OS using the English zpmt command and want to allow the display of Japanese characters correctly in your environment, you need to modify some script files.

1. Edit the setupCmdLine.sh file
   from: CONSOLE_ENCODING="-Dws.input.encoding=cp1047 -Dws.output.encoding=cp1047"
   to: CONSOLE_ENCODING="-Dws.input.encoding=cp1399 -Dws.output.encoding=cp1399"
2. Edit the wsadmin.sh file
   from: EXTRA_D_ARGS="-Dfile.encoding=ISO8859-1
   to: EXTRA_D_ARGS="-Dfile.encoding=IBM-932

Making these two changes will enable you to see the Japanese messages correctly.

zpmt command

The zpmt command that you run with the response file needs to conform to syntax that is outlined in this topic.

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
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 work space directory

-transfer
Copy 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.

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 that the user invoking zpmt.sh has r/w access to.

1. `zpmt.sh -workspace /xxx -transfer -allocate -responseFile /xxx/ZCellcmd.responseFile`
   This will:
   - Generate the customization jobs to the location specified by profilePath in the response file
   - Allocate the target CNTL and DATA datasets, using the high level qualifier specified by targetHLQ in the response file
   - Transfer the jobs from the file system to the CNTL and DATA datasets
2. `zpmt.sh -workspace /xxx -responseFile /xxx/ZAppSrvcmd.responseFile`
   This will generate the customization jobs to the location specified by profilePath in the response file.
3. `zpmt.sh -workspace /xxx -allocate -transfer -profilePath /xxx/ZAppSrvcmd`
   This will:
   - Allocate the target CNTL and DATA datasets, using the high level qualifier specified by targetHLQ in the response file
   - Transfer the generated jobs at the location specified by profile path to those datasets

   Note: This usage assumes the jobs have already been generated with a previous invocation of zpmt.sh
4. `zpmt.sh -workspace /xxx -transfer -responseFile /xxx/ZDmgrcmd.responseFile`
   This will transfer 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 zpmt.sh, and that the target CNTL and DATA datasets have already been allocated

Variables for configuring a standalone application server using the 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 a standalone application server.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zServantGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

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

System locations

System name (zSystemNane)
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

Note: 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

Note: 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

See “Product file system” on page 32 for more information.

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

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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 customization

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

Server customization

Short cell name (zCellShortName)
Name that identifies the cell to z/OS facilities such as SAF

Note:

- 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.

Note:

- 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

Note:

- 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.

Note:

- 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.

Note: 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.

Note:

- 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. See “Cataloged procedures” on page 54 for more information.

Note: 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. See “Cataloged procedures” on page 54 for more information.

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

Note: 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 customization

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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

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

Server TCP/IP information customization

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.

Note: 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

Note: 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 hostname 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

Note: Value cannot be 0.

HTTPS transport port (zHttpTransportSslPort)
Port for secure HTTP requests

Note: 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

Note: Value cannot be 0.

Service integration port (zServiceIntegrationPort)
Port for service-integration requests

Note: Value cannot be 0.

Service integration secure port (zServiceIntegrationSecurePort)
Port for secure service-integration requests

Note: Value cannot be 0.

Service integration MQ interoperability port (zServiceIntegrationMqPort)
Port for service-integration MQ interoperability requests

Note: Value cannot be 0.

Service integration MQ interoperability secure port (zServiceIntegrationSecureMqPort)
Port for secure service-integration MQ interoperability requests

Note: Value cannot be 0.

Session initiation protocol (SIP) port (zSessionInitiationPort)
Port for session initiation requests

Note: Value cannot be 0.

Session initiation protocol secure port (zSessionInitiationSecurePort)
Port for secure session initiation requests

Note: 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

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

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 *.

Note: 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 set a SAF profile 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). Enter a 1-8 SAF profile prefix.

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

Note: 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

Note: 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

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 install directory path (webServerInstallPath)
Varies by user configuration

Web server plugin install 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 configuring a deployment manager using the 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 a deployment manager.

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Note: Use the IBM default names the first time you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Server type

Server type (serverType)
Type of server to be created within this management profile

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zServantGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

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

System locations

System name (zSystemNane)
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

Note: 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

Note: 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

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

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

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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 customization

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

Server customization

Short cell name (zCellShortName)
Name that identifies the cell to z/OS facilities such as SAF

Note:

- 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:

- 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

Note:

- 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:

- 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.

Note: 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.

Note:

- 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.

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

Server address space information customization

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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 customization

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.

Note: 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

Note: 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 hostname 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

Note: 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

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

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 *.

Note: 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 set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (zSecurityDomainId)
Set this to `true` if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

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.

Note: 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

Note: 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

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 configuring a managed (custom) node using the 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 a managed (custom) node.

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Note: Use the IBM default names the first time that you install WebSphere Application Server for z/OS to make the installation instructions easier to follow.

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zServantGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

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

System locations

System name (zSystemNane)
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

Note: 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

Note: 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

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

Note: The minimum suggested size is 300 cylinders (3390).

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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 customization

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

Server customization

Short node name (zNodeShortName)
Name that identifies the node to z/OS facilities such as SAF

Note:

- 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.

Note:

- 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. See “Cataloged procedures” on page 54 for more information.

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

Note: 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 customization

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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

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

Node TCP/IP information customization

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

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

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.

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

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

Note: 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.

Note: 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.

Note: 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

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 federating an application server using the 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 federating an application serverr.

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Federation information

Profile name (profileName)
The profile name is `default`.

Profile path (profilePath)
Profile path

Template path (templatePath)
Template path

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 is it 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.

Note: 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

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

Configuration group name (zConfigurationGroup)
Group name of the WebSphere Application Server configuration group

Configuration user ID (zAdminUserid)
User ID that owns the configuration file system

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

See “Product file system” on page 32 for more 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

Application Server security enabled (zFederateAppServerSecurity)
This is required if global security is enabled on the cell containing the node that is being federated.

User ID (zFederateAppServerSecurityUserID
User ID with full administrative privileges for the cell containing the application server

Password (zFederateAppServerSecurityPassword)
Password for user ID

Include applications? (zFederateIncludeApps)
Specify `true` if you want to include applications with your deployment manager node. Enabling this option instructs the addNode program to include applications from the node, as it would remove them prior to federation otherwise. If the application already exists in the cell, a warning is printed and the application is not installed into the cell.

Note: You must use this option to migrate all the applications to the new cell. Federating the node to a cell using the addNode command does not merge any cell-level configuration information, including that from virtualHost.

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

Note: 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.

Note: 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.

Note: 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`.

Application server ORB port (zFederateAppServerOrbPort)
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

Note: Value cannot be 0.

Note: The add node operation creates the node agent administrative server with a default ORB port equivalent to the INS CosNaming default bootstrap port. Because this same port was previously used by the node's initial standalone server, the initial standalone server's ORB port must change to a new port value. The default value to which the application server's ORB port is set is 9810. If you configure multiple cells that intersect the same systems, use of the default value will cause a port conflict between these cells. This option helps you set the port number in case port 9810 was previously assigned.

Federate service integration busses that exist on this node? (zFederateFederateSib)
Specify `true` to federate service integration busses that exist on this node. Otherwise, specify `false`.

Job statement customization

Job statement 1 (zJobStatement1)

Job statement 2 (zJobStatement2)

Job statement 3 (zJobStatement3)

Job statement 4 (zJobStatement4)

Variables for configuring a Network Deployment cell with an application server using the 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 a Network Deployment cell with an application server.

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zServantGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

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

System locations

System name (zSystemNane)
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

Note: 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

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

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

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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

Note: 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

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zAppServerConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zAppServerConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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 system information

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

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

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

Deployment manager server customization

Short cell name (zCellShortName)
Name that identifies the cell to z/OS facilities such as SAF

Note:

- 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:

- 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

Note:

- 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:

- 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.

Note: 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.

Note:

- 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.

Note: 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

Note:

- 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.

Note: 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.

Note:

- 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.

Note:

- 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

Note: 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. See “Cataloged procedures” on page 54 for more information.

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 customization

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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

Note: 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.

Note: 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

Note: 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 hostname 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

Note: 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.

Note: 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)

Note: 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)

Note: Value cannot be 0.

HTTPS transport port (zAppServerHttpTransportSslPort)
Port for secure HTTP requests (WC_defaulthost_secure)

Note: 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)

Note: Value cannot be 0.

Service integration port (zAppServerServiceIntegrationPort)
Port for service-integration requests (SIB_ENDPOINT_ADDRESS)

Note: Value cannot be 0.

Service integration secure port (zAppServerServiceIntegrationSecurePort)
Port for secure service-integration requests (SIB_ENDPOINT_SECURE_ADDRESS)

Note: Value cannot be 0.

Service integration MQ interoperability port (zAppServerServiceIntegrationMqPort)
Port for service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_ADDRESS)

Note: Value cannot be 0.

Service integration MQ interoperability secure port (zAppServerServiceIntegrationSecureMqPort)
Port for secure service-integration MQ interoperability requests (SIB_MQ_ENDPOINT_SECURE_ADDRESS)

Note: Value cannot be 0.

Session initiation protocol (SIP) port (zAppServerSessionInitiationPort)
Port for session initiation requests (SIP_DEFAULTHOST)

Note: Value cannot be 0.

Session initiation protocol secure port (zAppServerSessionInitiationSecurePort)
Port for secure session initiation requests (SIP_DEFAULTHOST_SECURE)

Note: 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)

Note: 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.

Note: 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.

Note: 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

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

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 *.

Note: 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 set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (zSecurityDomainId)
Set this to `true` if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

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

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 install directory path (webServerInstallPath)
Varies by user configuration

Web server plugin install 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 configuring an administrative agent using the 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 an administrative agent.

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Server type

Server type (serverType)
Type of server to be created within this management profile

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zServantGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

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

System locations

System name (zSystemNane)
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

Note: 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

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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.

System information

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read "Product file system" on page 32 for more information.

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 `/wassmpe`.

Server customization

Short cell name (zCellShortName)
Name that identifies the cell to z/OS facilities such as SAF

Note:

- 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:

- 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

Note:

- 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:

- 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.

Note: 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.

Note:

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

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 customization

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

Note: 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

Note: 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

Note: 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

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

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.

Note: 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

Note: 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 hostname 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).

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

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

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 *.

Note: 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 set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (zSecurityDomainId)
Set this to `true` if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

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

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 configuring a job manager using the 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 a job manager.

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Server type

Server type (serverType)
Type of server to be created within this management profile

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Servant group (zServantGroup)

Allow OS security to assign GID (zServantGroupGID)
Specify * to allow operating-system security to assign the group ID.

Allow user-specified GID (zServantGroupGID)
Specify an ID to use a specific ID.

Local user group (zLocalUserGroup)

Allow OS security to assign GID (zLocalUserGroupGID)
Specify * to allow operating-system security to assign the group ID.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

System locations

System name (zSystemNane)
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

Note: 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

Note: 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

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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.

System information

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

Server customization

Short cell name (zCellShortName)
Name that identifies the cell to z/OS facilities such as SAF

Note:

- 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:

- 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

Note:

- 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:

- 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.

Note: 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.

Note:

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

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 customization

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

Note: 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

Note: 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

Note: 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

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

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.

Note: 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

Note: 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 hostname 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).

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

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

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 *.

Note: 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 set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (zSecurityDomainId)
Set this to `true` if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

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

Note: 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

Note: 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

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 configuring a secure proxy server using the zpmt command

The zpmt command uses the values that you specify in for the variables defined in a response file to create customization data and instructions for configuring a secure proxy server.

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

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

System locations

System name (zSystemNane)
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

Note: 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

Note: You can specify up to 44 characters for the dataset name.

Directory path name relative to mount point (zWasServerDir)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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 customization

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

Server customization

Short cell name (zCellShortName)
Name that identifies the cell to z/OS facilities such as SAF

Note:

- 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.

Note:

- Name must be 50 or fewer characters.
- 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

Note:

- 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.

Note:

- Name must be 50 or fewer characters.

- 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.

Note: 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.

Note:

- 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. See “Cataloged procedures” on page 54 for more information.

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

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. See “Cataloged procedures” on page 54 for more information.

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

Note: 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

Security level information

Proxy security level (securityLevel)

High Represents the highest level of proxy server security based on certain proxy server settings

Medium
Represents the mid-level of proxy server security based on certain proxy server settings

Low Represents the lowest level of proxy server security based on certain proxy server settings

Supported protocols (supportedProtocols)

Web Select to support Web protocol

SIP Select to support SIP protocol

Server address space information customization

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 application server controller

Note: 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

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

Server TCP/IP information customization

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.

Bootstrap port (zBootstrapPort)
Port for IIOP requests that acts as the bootstrap port for this server

Note: Value cannot be 0.

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 hostname 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.

HTTP transport port (zHttpTransportPort)
Port for HTTP requests

Note: Value cannot be 0.

HTTPS transport port (zHttptransportSslPort)
Port for secure HTTP requests

Note: 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).

Session initiation protocol (SIP) port (zSessionInitiationPort)
Port for session initiation requests

Note: Value cannot be 0.

Session initiation protocol secure port (zSessionInitiationSecurePort)
Port for secure session initiation requests

Note: 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

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

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 *.

Note: 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 set a SAF profile 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). Enter a 1-8 SAF profile prefix.

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

Note: 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

Note: 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

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 configuring a secure proxy administrative agent using the 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 a secure proxy administrative agent

Note: See the sample response file in the *app_server_root*/zOS-config/zpmt/samples directory.

Server type

Server type (serverType)
Type of server to be created within this management profile

Profile information

Profile name (profileName)
The profile name is `default`.

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 is it 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.

Note: 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

Note: 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.

Allow user-specified GID (zConfigurationGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zServantGroupGID)
Specify an ID to use a specific ID.

Note: 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.

Allow user-specified GID (zLocalUserGroupGID)
Specify an ID to use a specific ID.

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

System locations

System name (zSystemNane)
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

Note: You can specify up to 44 characters for the dataset name.

Directory path name relative to mount point (zWasServerDir)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

See “Product file system” on page 32 for more information.

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

Primary allocation in cylinders (zConfigHfsPrimaryCylinders)
Initial size allocation in cylinders for the above dataset

Note: The minimum suggested size is 420 cylinders.

Secondary allocation in cylinders (zConfigHfsSecondaryCylinders)
Size of each secondary extent in cylinders

Note: 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.

System information

Product file system directory (zSmpePath)
Name of the directory where WebSphere Application Server for z/OS files reside after installation

Read “Product file system” on page 32 for more information.

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 `/wassmpe`.

Server customization

Short cell name (zCellShortName)

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

Note:

- 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:

- 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

Note:

- 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:

- 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.

Note: Name must be seven or fewer 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.

Note:

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

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 customization

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

Note: Name must be seven or fewer 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

Note: 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

Note: Name must be seven or fewer 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

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

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.

Note: Value cannot be 0.

Bootstrap port (zBootstrapPort)
Port for IIOP requests that acts as the bootstrap port for this server (BOOTSTRAP_ADDRESS)

Note: 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).

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

Note: Name must be seven or fewer characters.

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 *.

Note: 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 set a SAF profile prefix and choose an administrator user ID as well as an unauthenticated (guest) user ID.

SAF profile prefix (zSecurityDomainId)
Set this to `true` if you wish to include a SAF profile prefix in certain SAF security checks (APPL, CBIND, EJBROLE). Enter a 1-8 SAF profile prefix.

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

Note: 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

Note: 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

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)

Using the installation verification test

Before you begin

You initially run the installation verification test (IVT), which verifies that WebSphere Application Server is configured correctly for your system, during customization of each of your systems. If you want to run the IVT at a time other than during initial customization, however, there are two methods from which you can choose.

Note: These options are now available when you are running a standalone application server configuration as well as after federating an application server.

Select either method to invoke the IVT:

- “Running the installation verification test with a job”
- “Running the installation verification test from a command line” on page 383

Running the installation verification test with a job

The installation verification test (IVT) can be run in three steps.

Before you begin

The application server must be running when you initiate the test.

1. Verify that the application server is running.
2. Confirm that the ivtApp application is installed and started.
3. Submit the job BBOWIVT.

Results

The IVT runs a series of verification tests and reports pass or fail status for each in the messages generated by the BBOWIVT job. The output is written to the job output for the submitted BBOWIVT JCL and to the *was_home*/profiles/default/logs/ivtClient.log file.

Running the installation verification test from a command line

You can run the installation verification test (IVT) to get reports on pass or fail status for each in the messages generated by the BBOWIVT job.

Before you begin

The application server must be running when you initiate the test.

1. Verify that the application server is running.
2. Confirm that the ivtApp application is installed and started.
3. From a command line, navigate to the *was_home*/bin directory.
4. Issue the following command:

   ivt.sh *server_name profile_name* -p *port_number* [-host *host_name*]

   where

   - *server_name* is the short name of the server.
   - *profile_name* is the name of the profile.
   - -p *port_number* is an argument that specifies the port number.
   - -host *host_name* is an optional argument that specifies the host name. If you do not specify a host name, the program will use the host-name value that is set in your TCP/IP hosts file.

   Example:

   ```
   /WebSphere/V7R0/AppServer/bin> ivt.sh serverj default -p 9080 -host myhost
   ```

Results

The IVT runs a series of verification tests and reports pass or fail status for each in the messages generated by the BBOWIVT job. The output is written to standard output and to the *was_home*/profiles/default/logs/ivtClient.log file.

switchModules command

You can use the switchModules command to switch a configuration between using load modules in the file system and using load modules in a dataset.

Location

The switchModules.sh shell script is located in the *smpe_install_root*/bin or *app_server_root*/bin directory.

Syntax

```
switchModules.sh target_was_home
                 target_mode
                 (target_dataset_name)
```

Parameters

target_was_home
Home directory of the node that is the target of the switch

target_mode
Mode to which to switch

FS Switch *target_was_home* to using libraries out of the file system.

DS Switch *target_was_home* to using libraries out of the dataset.

target_dataset_name
Name of the dataset out of which to use the libraries

This parameter is required when you specify a mode of DS for *target_mode*.

Chapter 10. Applying product maintenance

Maintaining WebSphere Application Server requires an in-depth knowledge of MVS service techniques and the product service stream. This is especially important in a high yield production environment where availability is of the utmost importance. Therefore, planning service and knowing how to best apply service are essential skills.

Before you begin

Contact the IBM Software Support Center for information about preventive service planning (PSP) upgrades for WebSphere Application Server for z/OS. For more information about PSP upgrades, see the *WebSphere Application Server for z/OS: Program Directory*. Although the *Program Directory* contains a list of required program temporary fixes (PTFs), the most current information is available from the IBM Software Support Center.

The z/OS System Modification Program Extended (SMP/E) program is used to apply product maintenance to WebSphere Application Server for z/OS. The WebSphere Application Server update installer is not used under z/OS. A set of scripts called the **post-installer**, a part of WebSphere Application Server for z/OS, is used to make any configuration file system changes that are required as a consequence of product-maintenance.

About this task

Use the following procedure whenever you want to apply a new service release to your system.

1. Decide whether to run the post-installer automatically or manually. See “Applying a service level or restoring to the previous accepted service level” on page 386 for more information.
2. Make copies of your product datasets and file system structure.
3. Ensure your deployment manager node is at the same or a later service level than the application server nodes.
4. Use SMP/E to apply the required maintenance to the copies of your product dataset and file system structure.

   Note: Notice if you receive WTOR message BBOO0286A when applying your service. This is significant because it means the service you installed contains defects that are not backwards-compatible and you must therefore run the backoutPTF.sh script if you want to backout the service later.
5. Stop the application servers and the WebSphere Application Server for z/OS location service daemon.
6. Stop CTRACE.
7. Switch to the newly serviced WebSphere Application Server for z/OS product datasets. You can do this one of two ways:
   a. Rename the new datasets to replace the old ones.
   b. Recatalog the product datasets if the names are identical, or change WebSphere Application Server for z/OS cataloged procedures to refer explicitly to the new datasets.

      Note: If you use new dataset names, you need to also handle program controls, so ensure you update the program control list.

   Verify that the MVS link list and APF list refer to the newly-serviced datasets.
8. If the WebSphere Application Server for z/OS runtime is loaded into the link pack area, delete the old modules and load the new ones, or IPL the system to load the new modules into the LPA.
9. Verify that the newly-serviced product file system is correctly mounted.

10. Perform any other migration actions as instructed in PTF or APAR cover letters.
11. Start the location service daemon and application servers.
12. Complete any necessary post-installation tasks. In particular, make sure that the post-installer is run (either automatically or manually) against each node in order to update the configuration file system to the new service level. For more information, refer to “Completing post-installation tasks after using SMP/E to apply a new service level” on page 387.

Results

You can maintain service to clients when upgrading the host cluster of WebSphere Application Server for z/OS.

If you roll back to a previous maintenance level of WebSphere Application Server, be sure to run the post-installer against each node to back out configuration file system changes before switching to the older service level. See “Completing post-installation tasks before using SMP/E to restore to the previous accepted service level” on page 389 for more information.

Applying a service level or restoring to the previous accepted service level

About this task

Service that is applied to the WebSphere Application Server for z/OS product datasets and product file systems occasionally requires corresponding changes to be made to the configuration file systems for existing application serving environments that configure at a lower service level. Most of these post-maintenance or post-installation updates can be performed automatically. This is done by the post-installer.

The WebSphere Application Server for z/OS post-installer is a set of scripts that can be used to:

- Automatically detect and apply post-PTF service
- Back out (uninstall) service from the configuration HFS when returning to an older service level

The post-installation process is performed at the node level and must run against each node’s WebSphere Application Server home directory after maintenance is applied to the product datasets and HFS, and before the node is started. For more information about the post-installer and how to use it to apply or back out service to the configuration HFS, see the following references:

- “Completing post-installation tasks after using SMP/E to apply a new service level” on page 387
- “Completing post-installation tasks before using SMP/E to restore to the previous accepted service level” on page 389

1. Perform the post-install process in ether of two ways.
   - Automatically by leaving the configured JCL statements in the controller cataloged procedures that start the post-installer

     A console message will be displayed whenever the post-installation detects service to be applied. In some cases, some post-installation steps might still have to be performed manually. The post-installer will detect these situations and refuse to start the server.
   - Manually

     You can run the post-installer yourself against each node’s WebSphere Application Server home directory after installing maintenance and before starting the nodes.
2. Optional: You might find it useful to set up a WLM rule to combat performance problems related to post-installation.

Completing post-installation tasks after using SMP/E to apply a new service level

About this task

This article describes post-installation tasks you complete after applying a new service level. See Chapter 10, “Applying product maintenance,” on page 385, for more information about applying service to WebSphere Application Server for z/OS.

The post-installation functionality includes actions you perform the first time the server is restarted after you install service with SMP/E. This applies to WebSphere Application Server for z/OS as well as WebSphere Business Integration Server Foundation for z/OS. Depending on your system restrictions, you can choose to initialize post-installation processing either automatically or manually.

Automatic mode, which is recommended, includes a new step that automatically launches the ″applyPTF.sh″ shell script in the server procedure. The applyPTF.sh script, which is located in your bin directory (*was_home*/bin, where *was_home* is the absolute path of the WebSphere runtime home directory), verifies that any pending post-installation actions are properly applied before starting the server.

Manual mode is necessary only if the automatic mode does not conform to your organization standards (if multistep procedures are not allowed for example), if there is something else in your configuration that prevents the applyPTF.sh shell script from running properly, or if you are applying a particular service release that requires manual intervention. Refer to the section below, ″Running the post installer manually,″ for more information.

Post-installtion processing executes under the controller proc, so it executes with the identity assigned to that particular proc. While that identity has sufficient authority to perform most file system actions required on the WebSphere runtime home directory, you cannot assume it to have the appropriate authority for your applyPTF.sh shell script. Therefore, you cannot perform any post-installationon that requires special authority by ″inline″ apply processing. You must manually perform any such apply processing in ″batch″ mode, running applyPTF.sh or the appropriate jobs from a user that has the needed authority to apply a particular action.

Note:

- Before you run applyPTF.sh, ensure that WebSphere Application Server for z/OS is running with code page IBM-1047. See “Preparing z/OS to run WebSphere Application Server” on page 39 for more information.
- When you launch the shell script from the server proc, it automatically runs in ″inline″ mode and can only apply service that qualifies as ″inline.″
- If batch service is delivered, you’ll find the needed user authority noted in the service level documentation.

You can run the post-installer either automatically or manually. Follow the set of steps below that applies to your circumstance.

- Run the post installer automatically. This is running under the authority of the WebSphere Admin ID.

  Classify BPXBATCH using the WLM Workload Classification Rules for OMVS work. Use the started task job names to classify this work into the appropriate service class. This facilitates more efficient execution in automatic mode.
- Run the post installer manually.
  1. Edit your server control process procedures (for example, BBO7ACR) to remove the BPXBATCH step that invokes the applyPTF.sh script.
  2. After rolling service to each system, run batch job BBOWAPLB for each standalone application server node, and run BBOWAPLD for each deployment manager node, and for each managed node.

What to do next

The post installer component enforces that certain actions are performed successfully and preconditions are met before applying service, otherwise, warnings or error messages result. If you launched the applyPTF.sh script from the server proc, the output is appended to the *was_home*/properties/service/logs/applyPTF.out file. If you run applyPTF.sh manually from the shell, the output goes right to stdout (on the shell from where the applyPTF.sh script was run) and WTO messages are issued. In the latter case, no output is appended to the applyPTF.log log file.

Whenever actions are performed on the runtime home directory, a log file is kept. When warnings or errors occur, the absolute path to the log file is displayed so that you can examine the details of the problem. The following is a list of common errors that might occur when the post installer (applyPTF.sh) applies service. The errors will most likely appear in the form of error codes on the console on which applyPTF.sh was issued.

The post installer ran and determined that SMP/E restored the SMP/E home directory to a previous level of service than that at which the WebSphere runtime home directory is running.
This occurs if you used SMP/E to restore to the previous accepted service level without first running the backoutPTF.sh shell script. The server will not start if it detects this condition, and post-installation action halts without applying service.

The post installer issued a warning message while installing service.
The WebSphere Application Server for z/OS multiproduct PTF post installer detected warnings that were issued during the application of post-installation service for the product listed. The application of service was successful, but the warning messages should be examined. The warning messages are listed in the log file in the HFS file that is specified in the message.

The post installer incurred an error and stopped processing.
The WebSphere Application Server for z/OS multiproduct PTF post installer encountered an error while installing service for the product indicated in the message. The details of the error are contained in the HFS log file that is specified in the message. When this happens, review the log and correct the error. The servers will not be permitted to start until the error is corrected.

The post installer encountered warnings while applying service.
The WebSphere Application Server for z/OS multiproduct PTF post installer detected warnings that were issued during the application of post-installation service. The warnings might have been issued while post-installation service was being applied for WebSphere Application Server for z/OS or any of the extension products that are installed. A BBOO0250W message should have already been issued for each product that encountered warnings when the post-installation service was applied.

Reply with `Continue` to continue starting the application server. Reply with `Cancel` to cancel starting the application server. Because service has already been completed, the multiproduct PTF post installer will not run again the next time the server is restarted.

Running the post installer manually.
As mentioned above, there are reasons why an organization might require the post installer to be run manually, also known as batch mode. The post installer will not allow post install service to be applied if a node is moved to a different system other than the system where it was configured. (In this case the WTO BBOO0287A will be issued) . Running the post installer in batch mode, however, will apply post install service to a node, even if it is now located on a system other than the one where it was originally configured.

The post installer can be invoked manually by using either of the two following procedures:

- Run the batch job that was created by the customization tool walkthrough (CNTL dataset) for each node. Use BBOWAPLB for standalone application server nodes and BBOWAPLD for Network Deployment cell nodes.
- Invoke the shell script directly. It is stored in the /bin directory of each node. From OMVS running under the authority of the WebSphere Admin ID, issue the `./applyPTF.sh batch` shell script.

Completing post-installation tasks before using SMP/E to restore to the previous accepted service level

About this task

This article describes those post-install tasks you might need to complete before using SMP/E to restore to the previous accepted service level.

If you install service and then find that, for some reason or another, you need to revert to a previous release, you typically need only to use SMP/E to restore to the previous accepted service level. However, some service releases contain defects that are incompatible with previous releases of WebSphere Application Server for z/OS.

Note: You will know if you are applying a service level that contains backward-incompatible defects if you receive message BBOO0286A (WTOR message 286) when the post installer applies the service. The console will prompt you to accept the backward-incompatible change. If you decide not to accept the change, you must either use SMP/E to roll back to the previous level or follow the post-install backout plans described in “Completing post-installation tasks after using SMP/E to apply a new service level” on page 387.

When you restore to the previous accepted service release, you need to first ″back off″ any post-installation actions containing backwards-incompatible defects that were applied during that service before using SMP/E to restore to the previous accepted service level. This article describes the steps necessary to run the backoutPTF.sh shell script, which is located in your bin directory (*was_home*/bin, where *was_home* is the absolute path of the WebSphere runtime home directory) and which handles the backing out of applied post-installation service for you.

1. Bring down those servers in the node for which you are doing back-off processing.
2. Launch the backoutPTF.sh script. You will need to specify the product and the committed service level to which you intend SMP/E to revert.

   Example: This is an example of the command used to run the backoutPTF.sh shell script, run from the shell by a user with the proper authority. It prepares the WebSphere Application Server for z/OS runtime home directory to run at service level ″o0511.05.″

   ```
   backoutPTF.sh WebSphere o0511.05
   ```

   Note: The shell script is case-sensitive.
3. After using the backoutPTF.sh shell script, follow the normal SMP/E procedures for restoring to the previous accepted service level.

Results

You know you are done when you are successfully back on the service level that you want.

What to do next

The following is a list of common errors that might occur when you use backoutPTF.sh to back out of service. The output goes right to stdout (on the shell from where the applyPTF.sh script was run).

A valid, currently installed PTF or APAR name and the target service level must be specified (case-sensitive).

If a PTF or APAR is not specified, then the ″usage″ of the command is printed.

Chapter 11. Troubleshooting installation and configuration

This article describes troubleshooting the installation of the WebSphere Application Server for z/OS product.

Before you begin

If an installation is not successful, use the troubleshooting information to correct the problems.

About this task

- For current information available from IBM Support on known problems and their resolution, see the IBM Support page.
- In order to avoid problems when you install, review the steps listed on the “Ensuring problem avoidance” page.
- If your application fails repeatedly during operations causing the application servants to terminate, workload management (WLM) might terminate the application environment for the application. Refer to “Handling workload management and server failures” on page 395 for more information.

What to do next

IBM Support has documents that can save you time gathering the information that you need to resolve a problem. Before opening a PMR, see the IBM Support page.

Ensuring problem avoidance

Before you begin

To implement WebSphere Application Server for z/OS, you must implement the necessary features, subsystems, and resources required for the runtime environment. This section provides checklists for tasks you should verify before running your WebSphere Application Server for z/OS system to prevent the most common errors encountered during the installation.

Before you begin: Perform the following steps to ensure problem avoidance, checking off each item as you complete it:

1. Prepare your z/OS environment:

Table 6.

Check off	Item
	Check that all the maintenance suggested in the PSP bucket WASAS700 subset H28W7000 has been applied.
	Make certain your address space is large enough. Some WebSphere Application Server for z/OS servers must be able to get a 1GB virtual region to run any workload. Make sure that your installation exits (IEFUSI) do not limit the virtual region size. We recommend that you specify REGION=0M so as not to limit their size.
	Add another local page dataset, two if your system does any paging of the WebSphere Application Server for z/OS server address spaces.

2. Prepare your DB2 subsystem (if you will use DB2):

Table 7.

Check off	Item
	Increase the MAX USERS (CTHREAD) and MAX BATCH CONNECT (IDBACK) in your DB2 environment settings. Use the sample job in DSN710.SDSNSAMP(DSNTEJ6Z) to display the ″ZPARMS″ settings of the running system. (An alternative is to use the DB2 Control Center to display these parameters.)
	Define at least 200 buffers to the DB2 BP32K buffer pool. Use this command to display the current bufferpool allocations: `-dis bpool(active)detail`. Verify JDBC 2.0 functionality. The JDBC IVT sample01 JAVA application does not exercise JDBC 2.0 drivers nor the RRS attach facility. A modified version that tests these functions can be found in the DB2 Conundrum white paper at http://www.ibm.com/support/techdocs/atsmastr.nsf/PubAllNum/WP100217. (This will also verify that the DSNJDBC plan is bound correctly and that it matches the .ser file.)
	Verify the level of DB2 code running on your system with the DSNTEJ6U sample job or run the DSNUTILB utility with the `DIAGNOSE DISPLAY MEPL` command. The module names, dates, and PTF number on the right of the report are in EBCDIC.
	Make sure that any updates to the DB2 ERLY code are installed, and that you have IPLed your system to activate them.

	Check the JDBC service installed on your system. Use the following Java program to display the service level:
	`export LIBPATH=/usr/lpp/db2/db2710/lib:$LIBPATH>`
	`java -cp /usr/lpp/db2/db2710/classes/db2j2classes.zip`
	`COM.ibm.db2os390.sqlj.util.DB2DriverInfo`
	
	The typical output message looks like this:
	`DB2 for OS/390 SQLJ/JDBC Driver build version is:DB2 7.1 PQ54756`

3. Verify your UNIX System Service configuration:

Table 8.

Check off	Item
	Specify enough threads, files, and processes in your BPXPRMxx member of parmlib. Here is a starting list if you do not have it set up yet: • MAXTHREADS: 10000 • MAXTHREADTASKS: 5000 • MAXFILEPROC: 10000 • MAXSOCKETS in the AF_INET domain: 12000 • SHRLIBRGNSIZE: 67000000 (134000000 recommended)
	If you have an exit that checks for valid accounting codes, you might need to specify an accounting value for spawned address spaces. Use the _BPX_ACCT_DATA= variable in the was.env file.
	Ensure that the user ID associated with running the installation jobs that run the BPXBATCH shell scripts has an OMVS segment that directs PROGRAM('/bin/sh') to use the z/OS shell rather than the tcsh (C) shell (at '/bin/tcsh'). These particular shell scripts will not run from the tcsh shell.

4. Plan your SMP/E tasks:

Table 9.

Check off	Item
	You can install WebSphere Application Server for z/OS into an SMP/E environment (SMP/E 3.1 or later) separate from the one you use for z/OS. This includes target and distribution zones, as well as HFS datasets. We recommend that you use a separate environment, but you should enable the cross-zone checking so that any prerequisite service requirement can be checked between the WebSphere Application Server for z/OS and z/OS SMP/E zones.
	Verify that the DDDEF for the LTS dataset describes a PDSE format dataset. This will avoid LINK-EDIT errors during the SMP/E processing.
	You should carefully read the *WebSphere Application Server for z/OS: Program Directory*. This is a very large product and you have to make sure that there is sufficient space in all target and temporary datasets for receive and apply processing.

5. Plan for the Profile Management Tool:

Table 10.

Check off	Item
	Install the WebSphere Customization Tools.
	Make sure that you have an FTP server running on your target z/OS system.
	Complete the worksheets for each area before beginning.

6. Check your TCP/IP configuration:

Table 11.

Check off	Item

	Telnet into UNIX Systems Services and issue these commands to verify that you can find your host name by IP address or IP host-name:
	• Get the local host name: `hostname`
	– You will get a response such as: sc49.itso.ibm.com
	– Use the output from the hostname command for the following `nslookup` command.
	• Get host address by name: `nslookup sc49.itso.ibm.com`
	– You will get a response such as this:
	`Server:sc49.itso.ibm.com`
	`Address:9.12.6.15`
	`Name:sc49.itso.ibm.com`
	`Addresses:9.12.6.15`
	– Use the dotted IP address from this display for the following command.
	• Get host name by address: `nslookup 9.12.6.15`
	– You will get a response such as in the previous nslookup display.
	There is also a small Java program, InetInfo.java, that you can run to verify the same TCP/IP configuration. See techdocs for the program at http://www.ibm.com/support/techdocs/atsmastr.nsf/PubAllNum/TD100609.
	Example: This example shows you how to run the InetInfo Java code.
	`JAVA4 @SC42:/u/java4>export PATH=/usr/lpp/java/IBM/J1.3/bin`
	`JAVA4 @SC42:/u/java4>java InetInfo`
	`get Local Host`
	`IP Address:9.12.6.27`
	`get Host Name By Address using 9.12.6.27`
	`Host Name:wtsc42oe.itso.ibm.com`
	`get Host Address By Name using wtsc42oe.itso.ibm.com`
	`Host Address:9.12.6.27`

	Issue the `hometest` command from TSO. It should show the correct TCP Host name, corresponding IP address(es), and HOME IP addresses. If it does not produce the correct results, then TCP/IP is not configured correctly.
	If the fully qualified TCP/IP HostName is greater than 24 characters, then a DNS will be required. Otherwise, the /etc/hosts file can provide the naming lookup.
	Verify that the DNS name you are using is definitive (authoritative) in your installation.

7. Verify that security is in place:

Table 12.

Check off	Item
	Check that the location service daemon has access to parmlib concatenation to retrieve CTRACE settings in the CTIBBOxx member.
	Verify that all WebSphere Application Server for z/OS servers must have READ access to any datasets or files in their JCL procedures.
	Verify that your installation has the RACF list-of-groups turned on. (SETROPTS LIST will show you if turned on or off.) Without this list of groups turned on, an ID cannot belong to more than one group and ASSR1 associates with only WSSR1 instead of both WSSR1 and WSCFG1. Use the command `SETROPTS GRPLIST` to turn on the list of groups.

Table 12. (continued)

Check off	Item
	Define the profile BPX.SAFFASTPATH in the FACILITY class to enable SAF fastpath support.
	Verify that the authorization bits for the WebSphere Application Server for z/OS HFS (default name is /usr/lpp/zWebSphere/V7R0) file are correctly set up for the WebSphere Application Server for z/OS configuration group.

8. Verify that product code is consistent:

Table 13.

Check off	Item
	After any maintenance has been applied, verify that the code loaded in LPALIB or LNKLST is synchronized with the code in the product file system. Check the location service daemon job log to verify that the correct maintenance level is in use.

You are done when you have checked all the applicable items.

Handling workload management and server failures

Before you begin

If your application fails repeatedly during operations causing the application servants to terminate, workload management (WLM) might terminate the application environment for the application. WebSphere Application Server for z/OS issues the following message if it tries to use a failed application environment:

```
BBOO0075E Unable to schedule work. WLM application environment applenv has stopped.
```

You need to fix the problem with your application, then restart the application environment with the RESUME option on the VARY WLM command.

About this task

Perform these steps to check and start the WLM application environment.

1. Display the application environment.
   Issue the following command:
   ```
   d wlm,dynappl=*
   ```
2. Start the application environment.
   Issue the following command:
   ```
   v wlm,dynappl=environment_name,resume
   ```
   where *environment_name* is the name of the application environment.

Results

You know that you have finished when a re-display of the application environment shows that it is available.

Installation problems

Select the problem that you are having with the WebSphere Application Server installation:
- The installation completes but the administrative console does not start.

IBM Support has documents and tools that can save you time gathering information needed to resolve problems. If you detect a problem, before opening a problem report see if the problem is a known problem by checking the Support page:
- http://www.ibm.com/software/webservers/appserv/zos_os390/support/

Post-installation notes on the error log

After installation is complete, use the administrative console to change the log stream name or create new log stream names for servers or servants.

Note:

- A server's error log stream setting overrides the general WebSphere Application Server for z/OS setting, and a servant setting overrides a server setting. Thus, you can set up general error logging, but direct error logging for servers or servants to specific log streams.
- If you create a new log stream name through the administrative console, you must configure a new log stream on z/OS and, if using the coupling facility, define a corresponding new coupling facility log stream.
- If you changed an existing log stream, or created a new one, you probably need to restart WebSphere Application Server for z/OS. When the name of a log stream is changed through the administrative console, in most cases a restart of WebSphere Application Server for z/OS is required before the change becomes effective. The only case when the change takes effect automatically is when the log stream name is changed for a server along with other changes that cause the server to be restarted.

If you want WebSphere Application Server for z/OS messages that occur during execution of a z/OS client to be recorded in an error log stream, code the `client_ras_logstreamname` WebSphere variable in its environment file then initialize the client. For more information about `client_ras_logstreamname` and the related variable `ras_log_logstreamName`, see the WebSphere variables in the administrative console or the information center.

Our RACF samples BBOWBRAC and BBODBRAC give UPDATE authority to the runtime control and servant user IDs for the log stream you created (they require that you supply a log stream name). If you want to grant access to the log stream after installation and configuration, perform the following actions:
- For each server identity that writes to the log stream (or client identity, if you allow clients to write to the error log stream), assign UPDATE access to the log stream.
- For each user who browses the error log stream, assign READ access.

Follow the sample RACF commands in BBOWBRAC or BBODBRAC.

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:

IBM Director of Intellectual Property & Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
USA

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Mail Station P300
2455 South Road
Poughkeepsie, NY 12601-5400
USA
Attention: Information Requests

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

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.