IBM WebSphere Process Server for Multiplatforms

IBM

Installing and Configuring WebSphere Process Server

Version 7.0.0

30 April 2010

This edition applies to version 7, release 0, modification 0 of WebSphere Process Server for Multiplatforms (product number 5724-L01) and to all subsequent releases and modifications until otherwise indicated in new editions.

To send us your comments about this document, send an e-mail message to doc-comments@us.ibm.com. We look forward to hearing from you.

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.

Contents

Tables

WebSphere Process Server: Product package contents

Learn how to acquire WebSphere® Process Server and what software is supplied in its media packs and downloadable electronic installation images.

How to acquire WebSphere Process Server

You can obtain the product code in any of the following ways:
- From the product media packs, which include CD-ROM and DVD media.
- From the Passport Advantage® site, where licensed customers can download installation images. For more information about the images available for download, see the Passport Advantage download document.

To buy the software, contact your IBM® representative or IBM reseller, or visit the WebSphere Process Server home page at http://www.ibm.com/software/integration/wps and select the *How to buy* link in the left column.

Software supplied with WebSphere Process Server

Each media pack includes software that you need to install WebSphere Process Server, to set up your WebSphere Process Server environment, and to assemble and deploy applications. Also included in each media pack are optional supplemental software programs that provide value and tool support for your production and development environments.

Table 1 lists the software that is provided with the WebSphere Process Server product. Not every software program is supplied on every platform.

Table 1. Software supplied with WebSphere Process Server

Software	Description
WebSphere Process Server	Based on service-oriented architecture (SOA) and as a single, simplified programming model, WebSphere Process Server is the next-generation business process server that delivers and supports all styles of integration based on open standards to automate business processes that span people, workflows, applications, systems, platforms, and architectures. Features new in this release of WebSphere Process Server can be found in the topic *What is new in this release* in the *WebSphere Process Server for Multiplatforms, V7.0 Product Overview* PDF. Or you can view the topic in the WebSphere Process Server for Multiplatforms, V7.0 online information center at http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/.
WebSphere Portal Add-in for WebSphere Process Server	WebSphere Portal provides Web-based client access to applications, as well as to human tasks and business processes enacted by WebSphere Process Server, through standard-based iWidget integration.

Table 1. Software supplied with WebSphere Process Server (continued)

Software	Description
WebSphere Application Server Network Deployment	The industry's premier Java™-based application platform, integrating enterprise data and transactions for the dynamic e-business world. The Network Deployment version, upon which WebSphere Process Server is built, delivers a rich application deployment environment with application services that provide enhanced capabilities for transaction management, as well as the security, performance, availability, connectivity, and scalability expected from the WebSphere family of products. This configuration also enables clustering, edge-of-network services, Web services enhancements, and high availability for distributed configurations. For more information about WebSphere Application Server Network Deployment, see theWebSphere Application Server Network Deployment information center.
IBM HTTP Server	The foundation of any e-business application is the Web server. IBM HTTP Server features include: • Easy installation • Support for SSL secure connections • Fast Response Cache Accelerator • IBM support as part of the WebSphere bundle • Hardware crypto support • Administration Server that helps to administer and configure IHS servers • Help information that uses the easy-to-navigate design that is common to all WebSphere products
Web server plug-ins	WebSphere Process Server supplies a unique binary plug-in module and an associated plug-in configuration file for each supported Web server. The Plug-ins Installation wizard installs required files and configures the Web server and the underlying application server of WebSphere Process Server to allow communication between the servers.
WebSphere Application Server Application Clients	An application client module is a Java Archive (JAR) file that contains a client for accessing a Java application. Running Java EE and Thin application clients that communicate with the underlying WebSphere Application Server product requires that elements of the Application Server are installed on the unit on which the client runs. However, if the system does not have the Application Server installed, you can install Application Clients, which provide a stand-alone client runtime environment for your client applications.
WebSphere Process Server Help System built on Eclipse	The WebSphere Process Server Help System is an Eclipse- and browser-based help system packaged for installation with WebSphere Process Server. WebSphere Process Server documentation is packaged for download as Eclipse document plug-ins, and can be viewed using this help system. Both the help system and document plug-in format are based on an open source approach developed by the Eclipse Project.

Table 1. Software supplied with WebSphere Process Server (continued)

Software	Description
WebSphere Application Server Edge Components	WebSphere Application Server Edge Components address the needs of highly available, high-volume environments. The Edge Components include sophisticated load balancing, caching, and centralized security capabilities. See the WebSphere Application Server Edge Components Web page for more information.
DB2® Restricted Enterprise Edition	DB2 Restricted Enterprise Edition includes portions of DB2 Enterprise Server Edition (DB2 Enterprise 9). DB2 Enterprise 9 is designed to meet the data server needs of mid- to large-size businesses. It can be deployed on Linux®, UNIX®, or Windows® servers of any size, from one processor to hundreds of processors. DB2 Enterprise 9 is an ideal foundation for building on demand enterprise-wide solutions. A broad array of autonomic or self-managing capabilities can free more administrator time to focus on driving business value. The ease of use in DB2 and the self-managing characteristics might even eliminate the need for dedicated administrators in smaller implementations. DB2 provides the following clients: • DB2 Runtime Client. This client is best suited for enabling applications to access DB2 servers. • DB2 Client. This client includes all the functionality found in the DB2 Runtime Client plus functionality for client-server configuration, database administration, and application development.
IBM Tivoli® Directory Server	The IBM Tivoli Directory Server product is a powerful Lightweight Directory Access Protocol (LDAP) infrastructure. Tivoli Directory Server provides a foundation for deploying comprehensive identity management applications and advanced software architectures. See IBM Tivoli Directory Server for more information.
IBM Tivoli Access Manager	IBM Tivoli Access Manager integrates with e-business applications right out of the box, to deliver a secure, unified, and personalized e-business experience. By providing authentication and authorization APIs and integration, Tivoli Access Manager helps you secure access to business-critical applications and data that might be spread across the extended enterprise. See IBM Tivoli Access Manager for e-business for more information.

Table 1. Software supplied with WebSphere Process Server (continued)

Software	Description
IBM Support Assistant	The IBM Support Assistant (ISA) is a tool that helps you use various IBM Support resources. The IBM Support Assistant offers four components to help you with software questions: • A Search component, which helps you access pertinent support information in multiple locations. • A Support Links component, which provides a convenient location to access various IBM Web resources such as IBM product sites, IBM support sites, and links to IBM news groups. • An Education component, which provides guided access to IBM product education Web sites, including IBM Education Assistant modules. • A Service component, which helps you submit an enhanced problem report that includes key system data to IBM. Using the IBM Support Assistant with WebSphere Process Server requires installing IBM Support Assistant, version 4.0.2, and then installing plug-ins for WebSphere Process Server.
IBM DMZ Secure Proxy Server for IBM WebSphere Application Server	IBM DMZ Secure Proxy Server for IBM WebSphere Application Server provides a secure platform for your proxy server. It allows you to install your proxy server in the demilitarized zone (DMZ), while reducing the security risk that might occur if you choose to install an application server in the DMZ to host a proxy server.
IBM WebSphere Installation Factory	IBM WebSphere Installation Factory creates installation packages for installing WebSphere Application Server in a reliable and repeatable way, tailored to your specific needs. The Installation Factory can produce two kinds of packages, a customized installation package (CIP) and an integrated installation package (IIP). A CIP is used to install a WebSphere Application Server product in addition to maintenance, profile customization, and user-defined scripting. An IIP is a larger package that can install an entire WebSphere software stack, such as an application server, a feature pack, and other user files.
IBM Rational® Application Developer Assembly and Deployment Features for WebSphere Software V7.5	IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 extends Eclipse with visual development features. It helps Java developers to rapidly design, develop, assemble, test, profile, and deploy high quality Java J2EE, Portal, Web/Web 2.0, Web services, and SOA applications.
IBM Rational Agent Controller V8.0	IBM Rational Agent Controller is a daemon that allows client applications to launch and manage local or remote applications and provides information about running applications to other applications.

Table 1. Software supplied with WebSphere Process Server (continued)

Software	Description
IBM Tivoli Composite Application Manager for WebSphere	IBM Tivoli Composite Application Manager for WebSphere helps increase performance in business-critical applications. It provides real-time problem detection, analysis, and repair to help maintain the availability and performance of on demand applications.

Media packs supplied with WebSphere Process Server

Seven media packs are available for WebSphere Process Server. Each media pack contains the product media applicable to a specific operating environment.

Note: Each media pack contains a WebSphere Process Server V7.0 Quick Start CD. This CD-ROM contains the WebSphere Process Server Quick Start Guide in all available translations.

See the following sections for detailed contents per platform:

AIX® media pack

The WebSphere Process Server for AIX media pack contains WebSphere Process Server content for both 32-bit and 64-bit platforms. Table 2 shows the content for 32-bit platforms. Table 3 on page 7 shows the content for 64-bit platforms.

Table 2. Contents of AIX media pack for 32-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for AIX 32-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for AIX 32-bit	One DVD

Table 2. Contents of AIX media pack for 32-bit platforms (continued)

Media label	How supplied
WebSphere Application Server Network Deployment V7.0 Supplements for AIX on PowerPC 32-bit	Two CD-ROMs contain the following installable components: • Application Client for WebSphere Application Server • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for AIX 32-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for AIX 32/64-bit	One DVD
IBM Tivoli Access Manager for e-business V6.1 for AIX 32/64-bit	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for AIX	One DVD
IBM Data Server Runtime Client V9.5 for AIX	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for AIX	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM WebSphere Installation Factory V7.0 for AIX on PowerPC® 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Table 2. Contents of AIX media pack for 32-bit platforms (continued)

Media label	How supplied
IBM Support Assistant V4.0.2 (Agent) for AIX on x86 32-bit	One CD-ROM

Table 3. Contents of AIX media pack for 64-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for AIX 64-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • IBM WebSphere Process Server Help System in the `IEHS` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for AIX 64-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for AIX on PowerPC 64-bit	Two CD-ROMs contain the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for AIX 64-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for AIX 32/64-bit	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM Tivoli Access Manager for e-business V6.1 for AIX 32/64-bit	One CD-ROM

Table 3. Contents of AIX media pack for 64-bit platforms (continued)

Media label	How supplied
IBM Tivoli Directory Server V6.2 AIX 64-bit	One DVD
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for AIX	One DVD
IBM Data Server Runtime Client V9.5 for AIX	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for AIX	One DVD
IBM WebSphere Installation Factory V7.0 for AIX on PowerPC 64-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

HP-UX media pack

The WebSphere Process Server for HP-UX media pack contains WebSphere Process Server content for both 32-bit and 64-bit platforms. Table 4 shows the content for 32-bit platforms. Table 5 on page 10 shows the content for 64-bit platforms.

Table 4. Contents of HP-UX media pack for 32-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for HP-UX 32-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for HP-UX on PA-RISC 32-bit	One DVD

Table 4. Contents of HP-UX media pack for 32-bit platforms (continued)

Media label	How supplied
WebSphere Application Server Network Deployment V7.0 Supplements for HP-UX on PA-RISC 32-bit	Two CD-ROMs contain the following installable components: • Application Client for WebSphere Application Server • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for HP-UX 32-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for HP-UX 32/64-bit	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Access Manager for e-business V6.1 for HP-UX 32/64-bit	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for HP-UX on HP Integrity Itanium-based systems	One DVD
IBM Data Server Runtime Client V9.5 for HP-UX on HP Integrity Itanium-based systems	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for HP-UX on HP Integrity Itanium-based systems	One DVD
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM WebSphere Installation Factory V7.0 for HP-UX 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM

Table 4. Contents of HP-UX media pack for 32-bit platforms (continued)

Media label	How supplied
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Table 5. Contents of HP-UX media pack for 64-bit platforms

Media label	How supplied
WebSphere Process Server for V7.0 HP-UX IA64	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for HP-UX on IA64 64-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for HP-UX on Integrity 64-bit	Two CD-ROMs contain the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for HP-UX 64-bit	One CD-ROM
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM Tivoli Access Manager for e-business V6.1 for HP-UX 32/64-bit	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM

Table 5. Contents of HP-UX media pack for 64-bit platforms (continued)

Media label	How supplied
IBM DB2 Enterprise Server Edition V9.5 for HP-UX on HP Integrity Itanium-based systems	One DVD
IBM Data Server Runtime Client V9.5 for HP-UX on HP Integrity Itanium-based systems	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for HP-UX on HP Integrity Itanium-based systems	One DVD
IBM Tivoli Directory Server V6.2 for HP-UX IA64	One CD-ROM
IBM WebSphere Installation Factory V7.0 for HP-UX 64-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Linux x86 media pack

The WebSphere Process Server for Linux x86 media pack contains WebSphere Process Server content for both 32-bit and 64-bit platforms. Table 6 shows the content for 32-bit platforms. Table 7 on page 13 shows the content for 64-bit platforms.

Table 6. Contents of Linux x86 media pack for 32-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Linux x86 32-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • IBM WebSphere Process Server Help System in the `IEHS` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Linux on x86 32-bit	One DVD

Table 6. Contents of Linux x86 media pack for 32-bit platforms (continued)

Media label	How supplied
WebSphere Application Server Network Deployment V7.0 Supplements for Linux x86 32-bit	Two CD-ROMs contain the following installable components: • Application Client for WebSphere Application Server • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WebSphere Application Server Network Deployment Rational Agent Controller V8.0	One CD-ROM
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Linux x86 32-bit	One CD-ROM
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Linux 32/64-bit	One DVD
IBM Tivoli Access Manager for e-business V6.1 for Linux 32/64-bit	One CD-ROM
IBM Tivoli Composite Application Manager for WebSphere V7.0 for Linux 32-bit, Multilingual	One CD-ROM
IBM Data Server Runtime Client V9.5 for Linux on 32-bit AMD and Intel® systems (x86)	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for Linux on 32-bit AMD and Intel systems (x86)	One DVD
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM WebSphere Installation Factory V7.0 for Linux on x86 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM

Table 6. Contents of Linux x86 media pack for 32-bit platforms (continued)

Media label	How supplied
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (Agent) for Linux on x86 32-bit	One CD-ROM

Table 7. Contents of Linux x86 media pack for 64-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Linux x86 64-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Linux on x86 64-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for Linux 64-bit	Two CD-ROMs contain the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
IBM DMZ Secure Proxy Server V7.0 for Linux x86 64-bit	One CD-ROM
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Linux 32/64-bit	One DVD
IBM Data Server Runtime Client V9.5 for Linux on AMD64 and Intel EM64T systems (x64)	One DVD
IBM DB2 Enterprise Server Edition V9.5 for Linux on AMD64 and Intel EM64T systems (x64)	One DVD
IBM Data Server Runtime Client V9.5 for Linux on AMD64 and Intel EM64T systems (x64)	One DVD

Table 7. Contents of Linux x86 media pack for 64-bit platforms (continued)

Media label	How supplied
IBM Data Server Client V9.5 for Linux on AMD64 and Intel EM64T systems (x64)	One DVD
IBM DB2 Enterprise Server Edition V9.5 for Linux on AMD64 and Intel EM64T systems (x64)	One DVD
IBM Tivoli Access Manager for e-business V6.1 for Linux 32/64-bit	One CD-ROM
IBM Tivoli Composite Application Manager for WebSphere V7.0 for Linux 64-bit, Multilingual	One CD-ROM
IBM Tivoli Directory Server V6.2 for Linux x86 64-bit	One DVD
IBM WebSphere Installation Factory V7.0 for Linux on x86 64-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Linux POWER® media pack

The WebSphere Process Server for Linux POWER media pack contains WebSphere Process Server content for both 32-bit and 64-bit platforms. Table 8 shows the content for 32-bit platforms. shows the content for 64-bit platforms.

Table 8. Contents of Linux POWER media pack for 32-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Linux PowerPC 32-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and , *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Linux on POWER 32-bit	One DVD

Table 8. Contents of Linux POWER media pack for 32-bit platforms (continued)

Media label	How supplied
WebSphere Application Server Network Deployment V7.0 Supplements for Linux PowerPC	Two CD-ROMs contain the following installable components: • Application Client for WebSphere Application Server • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Linux on PowerPC 32-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Linux PowerPC 32/64-bit	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Access Manager for e-business V6.1 Linux PowerPC 32/64-bit	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Linux on POWER (System i® and System p®) systems	One DVD
IBM Data Server Runtime Client V9.5 for Linux on POWER (System i and System p) systems	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for Linux on POWER (System i and System p) systems	One DVD
IBM WebSphere Installation Factory V7.0 Linux on PowerPC 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM

Table 8. Contents of Linux POWER media pack for 32-bit platforms (continued)

Media label	How supplied
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (Agent) for Linux on x86 32-bit	One CD-ROM

Table 9. Contents of Linux POWER media pack for 64-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Linux PowerPC 64-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Linux on POWER 64-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for Linux PowerPC 64-bit	Two CD-ROMs contain the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
IBM DMZ Secure Proxy Server V7.0 for Linux on PowerPC 64-bit	One CD-ROM
IBM Tivoli Directory Server V6.2 for Linux PowerPC 64-bit	One DVD
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Linux PowerPC 32/64-bit	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Linux on POWER (System i and System p) systems	One DVD

Table 9. Contents of Linux POWER media pack for 64-bit platforms (continued)

Media label	How supplied
IBM Tivoli Access Manager for e-business V6.1 for Linux PowerPC 32/64-bit	One CD-ROM
IBM WebSphere Installation Factory V7.0 for Linux on PowerPC 64-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Linux on System z® media pack

The WebSphere Process Server for Linux on System z media pack contains WebSphere Process Server content for both 32-bit and 64-bit platforms. Table 10 shows the content for 32-bit platforms. Table 11 on page 18 shows the content for 64-bit platforms.

Table 10. Contents of Linux on System z media pack for 31-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Linux on System z 31-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Application Server Network Deployment V7.0 Supplements for Linux on System z	Two CD-ROMs contain the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Linux on System z 31-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Linux on System z 32/64-bit	One DVD

Table 10. Contents of Linux on System z media pack for 31-bit platforms (continued)

Media label	How supplied
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Access Manager for e-business V6.1 for Linux PowerPC on System z 31/64-bit	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Linux on System z	One DVD
IBM Data Server Runtime Client V9.5 for Linux on System z	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for Linux on System z	One DVD
IBM Tivoli Composite Application Manager for WebSphere Application Server V7.0 for Linux 32/64-bit	One CD-ROM
IBM WebSphere Installation Factory V7.0 for Linux on System z 31-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Table 11. Contents of Linux on System z media pack for 64-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Linux on System z 64-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.

Table 11. Contents of Linux on System z media pack for 64-bit platforms (continued)

Media label	How supplied
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Linux on System z 64-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for Linux on System z 64-bit	Two CD-ROMs contain the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
IBM DMZ Secure Proxy Server V7.0 for Linux on System z 64-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Linux on System z 32/64-bit	One DVD
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Linux on System z	One DVD
IBM Data Server Runtime Client V9.5 for Linux on System z	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for Linux on System z	One DVD
IBM Tivoli Access Manager for e-business V6.1 for Linux PowerPC on System z 32/64-bit	One CD-ROM
IBM Tivoli Directory Server V6.2 Linux on System z 64-bit	One DVD
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Linux on System z 32/64-bit	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Composite Application Manager for WebSphere V7.0 for Linux PowerPC on System z 64-bit	One CD-ROM

Media label	How supplied
IBM WebSphere Installation Factory V7.0 for Linux on System z 64-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Solaris media pack

The WebSphere Process Server for Solaris media pack contains WebSphere Process Server content for SPARC 32-bit and 64-bit platforms and AMD 64-bit platforms. Table 12 shows the content for SPARC 32-bit platforms. Table 13 on page 22 shows the content for SPARC 64-bit platforms. Table 14 on page 23 shows the content for AMD 64-bit platforms.

Table 12. Contents of Solaris media pack for SPARC 32-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Solaris on SPARC 32-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Solaris on SPARC 32-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for Solaris SPARC 32-bit	Two CD-ROMs contain the following installable components: • Application Client for WebSphere Application Server • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Solaris SPARC 32-bit	One CD-ROM

Table 12. Contents of Solaris media pack for SPARC 32-bit platforms (continued)

Media label	How supplied
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Solaris on SPARC 32/64-bit	One DVD
IBM Tivoli Access Manager for e-business V6.1 for Solaris SPARC 32/64-bit	One CD-ROM
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Data Server Runtime Client V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM WebSphere Installation Factory V7.0 Solaris on SPARC 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (Agent) for Solaris on SPARC 32-bit	One CD-ROM

Table 13. Contents of Solaris media pack for SPARC 64-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Solaris SPARC 64-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Solaris on SPARC 64-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for Solaris SPARC 64-bit	Two CD-ROMs contain the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Solaris on UltraSPARC systems	One DVD
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM Data Server Runtime Client V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Solaris SPARC 64-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Solaris on SPARC 32/64-bit	One DVD

Table 13. Contents of Solaris media pack for SPARC 64-bit platforms (continued)

Media label	How supplied
IBM Tivoli Directory Server V6.2 for Solaris SPARC 64-bit	One DVD
IBM WebSphere Installation Factory V7.0 Solaris on SPARC 64-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Table 14. Contents of Solaris media pack for AMD 64-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Solaris AMD 64-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Solaris on AMD 64-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for Solaris AMD 64-bit	Two CD-ROMs contains the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Solaris on x64 systems	One DVD
IBM DB2 Enterprise Server Edition V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Data Server Runtime Client V9.5 for Solaris x64	One DVD

Table 14. Contents of Solaris media pack for AMD 64-bit platforms (continued)

Media label	How supplied
IBM Data Server Runtime Client V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Data Server Drivers V9.5 for AIX, HP-UX, Solaris, Linux, and Windows	One DVD
IBM Data Server Client V9.5 for Solaris x64	One DVD
IBM Data Server Client V9.5 for Solaris on UltraSPARC systems	One DVD
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Solaris AMD 64-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Solaris AMD 64-bit	One DVD
IBM Tivoli Access Manager for e-business V6.1 for Solaris AMD 64-bit	One CD-ROM
IBM Tivoli Directory Server V6.2 Solaris AMD 64-bit	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM WebSphere Installation Factory V7.0 for Solaris AMD 64-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

Windows media pack

The WebSphere Process Server for Windows media pack contains WebSphere Process Server content for both 32-bit and 64-bit platforms. Table 15 on page 25 shows the content for 32-bit platforms. Table 16 on page 26 shows the content for 64-bit platforms.

Table 15. Contents of Windows media pack for 32-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Windows 32-bit	One DVD contains the following installable components: • WebSphere Process Server in the `WBI` directory • IBM WebSphere Process Server Help System in the `IEHS` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Windows 32-bit	One DVD
WebSphere Application Server Network Deployment V7.0 Supplements for Windows on Intel 32-bit	Two CD-ROMs contain the following installable components: • Application Client for WebSphere Application Server • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WebSphere Application Server Network Deployment Rational Agent Controller V8.0	One CD-ROM
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Windows 32-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Windows 32/64-bit	One CD-ROM
IBM Tivoli Access Manager for e-business V6.1 for Windows 32/64-bit	One CD-ROM
IBM Tivoli Directory Server V6.2 for Windows 32/64-bit	One DVD
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM DB2 Enterprise Server Edition V9.5 for Windows on 32-bit AMD and Intel systems (x86)	One DVD

Table 15. Contents of Windows media pack for 32-bit platforms (continued)

Media label	How supplied
IBM Data Server Runtime Client V9.5 for Windows on 32-bit AMD and Intel systems (x86)	One DVD
IBM Data Server Drivers V9.5 for Windows on 32-bit AMD and Intel systems (x86)	One DVD
IBM Data Server Client V9.5 for Windows on 32-bit AMD and Intel systems (x86)	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM WebSphere Installation Factory V7.0 Windows on x86 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (Agent) for Windows on x86 32-bit	One CD-ROM

Table 16. Contents of Windows media pack for 64-bit platforms

Media label	How supplied
WebSphere Process Server V7.0 for Windows 64-bit	Two DVDs contain the following installable components: • WebSphere Process Server in the `WBI` directory • Migration tool in the `Migration` directory • WebSphere Application Server Network Deployment (V7.0) in the `WAS` directory. Use the Launchpad application in the root directory to install and view information about any of the installable components on the *WebSphere Process Server V7.0 DVD* and *WebSphere Application Server Network Deployment Supplements V7.0* CDs.
WebSphere Portal Add-in for WebSphere Process Server V7.0 for Windows 64-bit	One DVD

Table 16. Contents of Windows media pack for 64-bit platforms (continued)

Media label	How supplied
WebSphere Application Server Network Deployment V7.0 Supplements for Windows AMD 64-bit	One CD-ROM contains the following installable components: • IBM HTTP Server • IBM Support Assistant • Web Server Plug-ins • Migration tool
WorldType Fonts for Multiplatform, Multilingual for WebSphere Application Server Network Deployment V7.0 32/64-bit	One CD-ROM
IBM DMZ Secure Proxy Server V7.0 for Windows 64-bit	One CD-ROM
IBM Edge Components and IBM Edge Components for IPv6 V7.0 for Windows 32/64-bit	One DVD
IBM Tivoli Access Manager for e-business V6.1 for Windows 32/64-bit	One CD-ROM
IBM DB2 Restricted Enterprise Server Edition V9.5 - Authorized User Option - Activation CD	One CD-ROM
IBM Tivoli Directory Server V6.2 for Windows 32/64-bit	One DVD
IBM DB2 Enterprise Server Edition V9.5 for Windows on AMD64 and Intel EM64T systems (x64)	One DVD
IBM Data Server Runtime Client V9.5 for Windows on AMD64 and Intel EM64T systems (x64)	One DVD
IBM Data Server Drivers V9.5 for Windows on AMD64 and Intel EM64T systems (x64)	One DVD
IBM Data Server Client V9.5 for Windows on AMD64 and Intel EM64T systems (x64)	One DVD
IBM Rational Application Developer Assembly and Deployment Features for WebSphere Software V7.5 32/64-bit	Six CD-ROMs
IBM Tivoli Composite Application Manager for WebSphere V7.0 for UNIX-AIX, HP-UX and Solaris	One CD-ROM
IBM WebSphere Installation Factory V7.0 Windows on x86 64-bit	One CD-ROM

Table 16. Contents of Windows media pack for 64-bit platforms (continued)

Media label	How supplied
IBM Support Assistant V4.0.2 (WorkBench) for Linux 32-bit	One CD-ROM
IBM Support Assistant V4.0.2 (WorkBench) for Windows 32-bit	One CD-ROM

IBM Message Service Client for C/C++ and IBM Message Service Client for .NET are no longer part of the media packs. The latest versions of these products can be downloaded from the IBM Support and Download Web site at IA94: IBM Message Service Client for C/C++ and IA9H: IBM Message Service Client for .NET.

Limited use of IBM Tivoli Federated Identity Manager by WebSphere customers can be accessed at Tivoli Federated Identity Manager for WebSphere Application Server Network Deployment.

Preparing to install WebSphere Process Server

Before you install WebSphere Process Server, you must ensure that your system meets all the hardware and software requirements, and you must prepare your operating system for installation. You also need to decide whether to create a stand-alone server or a network deployment scenario and plan the configuration details needed.

About this task

The sub-topics contain information about preparing to install WebSphere Process Server in new and existing environments. Use the information to choose whether to create a stand-alone server or network deployment scenario and to consider any effects on your existing environment.

What to do next

Follow the instructions under "Installing the software" on page 41 to install the software.

Prerequisites for installing WebSphere Process Server

Before installing WebSphere Process Server or the WebSphere Process Server Client, you must ensure that a series of prerequisites have been met.

The prerequisites are:
- Plan your installation.

  For more information about planning your installation and about the databases required by WebSphere Process Server, see Planning for WebSphere Process Server and the topics under Determining your software needs.
- Ensure that your system meets all hardware and software requirements and that you have enough space (including temporary space) for your installation. See http://www.ibm.com/support/docview.wss?uid=swg27006205 for more information.
- When you start the installation process using the launchpad application and are installing the product together with a new installation of WebSphere Application Server Network Deployment, the launchpad installs IBM Installation Manager (if it is not already installed), WebSphere Application Server Network Deployment, WebSphere Application Server Feature Pack for XML, WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature, and WebSphere Process Server. See "Installing WebSphere Process Server interactively for the first time" on page 43 for more information.
- The WebSphere Integration Developer product comes with a default integration test client. If you plan to use this installation of WebSphere Process Server as the integration test client instead, refer to Planning to install WebSphere Process Server for use by WebSphere Integration Developer for information on how to set up this scenario.
- Prepare your operating system for installation. See Preparing the operating system for product installation in the WebSphere Application Server Network Deployment information center for links to platform-specific information.

- If you plan to install WebSphere Process Server over an existing installation of WebSphere Application Server or WebSphere Application Server Network Deployment, ensure that the product architectures match. You cannot install a 32–bit version of WebSphere Process Server over a 64–bit version of WebSphere Application Server or WebSphere Application Server Network Deployment; you cannot install a 64–bit version of WebSphere Process Server over a 32–bit version of WebSphere Application Server or WebSphere Application Server Network Deployment.
- If you plan to install from images obtained from Passport Advantage, see "Special considerations when installing from Passport Advantage" on page 139 for guidelines concerning user permissions and directory setup.
- Stop all server, deployment manager, and node agent processes on any products for which you intend to add features, or that you plan to extend. For instructions on how to perform these tasks, see "Stopping servers and nodes."
- Uninstall all maintenance packages on products you intend to add features to or that you plan to extend. Do this because features and components necessary to convert the products have not had any maintenance applied to them. If you remove all maintenance packages, your entire product will be at the same release level. You can then reapply the maintenance packages.
- Linux **On Linux platforms:** Ensure that your WebSphere Process Server installation has the following items:
  - Kernel and C runtime library
  - Current and all compatibility versions of the C++ runtime library
  - X Window libraries and runtime
  - GTK runtime libraries

If the prerequisites are satisfied, you are ready to install the product.

Stopping servers and nodes

You must stop all server, deployment manager, and node agent processes on any products for which you intend to add features or that you plan to extend or uninstall.

About this task

You use specific commands to stop server, deployment manager, and node agent processes. Perform the following steps to stop these processes:

Procedure

1. If you have one or more deployment managers installed, stop each *dmgr* process with the **stopManager** command. For example, issue one of the following commands, depending on your platform (where *profile_root* represents the installation directory of the deployment manager profile):
   - Linux UNIX **On Linux and UNIX platforms:** *profile_root*/bin/stopManager.sh
   - Windows **On Windows platforms:** *profile_root*\bin\stopManager.bat

   If security is enabled, use one of the following commands instead:
   - Linux UNIX **On Linux and UNIX platforms:** *profile_root*/bin/stopManager.sh -user *user_ID* -password *password*

- `Windows` **On Windows platforms:** *profile_root*\bin\stopManager.bat -user *user_ID* -password *password*

2. Stop node agent processes with the **stopNode** command. If you have nodes federated to deployment managers on your system, stop each node agent process that might be running on each server with a federated node. For example, issue one of the following commands to stop the node agent process, depending on your platform (where *profile_root* represents the installation directory of the federated node):

   - `Linux` `UNIX` **On Linux and UNIX platforms:** *profile_root*/bin/stopNode.sh

   - `Windows` **On Windows platforms:** *profile_root*\bin\stopNode.bat

   If servers are running and security is enabled, use one of the following commands instead:

   - `Linux` `UNIX` **On Linux and UNIX platforms:** *profile_root*/bin/stopNode.sh -user *user_ID* -password *password*

   - `Windows` **On Windows platforms:** *profile_root*\bin\stopNode.bat -user *user_ID* -password *password*

3. Stop each running stand-alone server with the **stopServer** command. Stop all server processes in all profiles on the server. For example, issue one of the following commands to stop the server in the profile, depending on your platform. In this example, *profile_root* represents the installation location of the profile:

   - `Linux` `UNIX` **On Linux and UNIX platforms:** *profile_root*/bin/stopServer.sh *server1*

   - `Windows` **On Windows platforms:** *profile_root*\bin\stopServer.bat *server1*

   If servers are running and security is enabled, use one of the following commands instead:

   - `Linux` `UNIX` **On Linux and UNIX platforms:** *profile_root*/bin/stopServer.sh *server1* -user *user_ID* -password *password*

   - `Windows` **On Windows platforms:** *profile_root*\bin\stopServer.bat *server1* -user *user_ID* -password *password*

What to do next

You can now add features to, extend, or uninstall the WebSphere product.

Creating the Common database manually before product installation

Use these instructions if you decide to create the Common database manually.

About this task

WebSphere Process Server provides default scripts that you can use to create the Common database manually. You might want to create the database manually in the following situations:

- If your organization requires that the database be created by a user with DBA privileges, that user must create the Common database before creating or augmenting profiles.

- If you intend to create or augment profiles during product installation, a user with DBA privileges must create the Common database before you install WebSphere Process Server.

Procedure

1. Go to the directory that contains the database creation scripts. The scripts are located both on the product media and in a directory after product installation. By default, the scripts are located in the following directories:

   - Location on the product media:

     – `Linux` `UNIX` *<media_root>*/dbscripts or *<extract_directory>*/ dbscripts

     – `Windows` *<media_root>*\dbscripts or *<extract_directory>*\dbscripts

   - Location after installation:

     – `Linux` `UNIX` *install_root*/dbscripts

     – `Windows` *install_root*\dbscripts

2. Open the directory containing the Common database scripts for your database product. The default location depends on the platform:

   - `Linux` `UNIX` `.../CommonDB/`*db_type*

   - `Windows` `...\CommonDB\`*db_type*

   The variable *db_type* represents the supported database type. Refer to Table 17 to locate your database type and directory name.

   Applicable database types and their directory names are as follows:

Table 17. Applicable database types and their directory names

Database type	Directory name	Corresponding subtopic
DB2 for i5/OS® (Toolbox) and DB2 for IBM i (Toolbox)	`DB2iSeries`	"Creating the DB2 for IBM i database"
DB2 Universal Database™ (for all operating systems except z/OS®)	`DB2`	"Creating the DB2 database" on page 34
DB2 for z/OS Version 8.x	`DB2zOSV8`	"Creating the DB2 database for z/OS" on page 35
DB2 for z/OS Version 9.x	`DB2zOSV9`	
Informix®	`Informix`	"Creating the Informix database" on page 37
Oracle	`Oracle`	"Creating the Oracle database" on page 38
Microsoft® SQL Server	`SQLServer`	"Creating the Microsoft SQL Server database" on page 39

3. Click the corresponding subtopic link in Table 17 to proceed with creating the common database manually.

Creating the DB2 for IBM i database

In order to create a Common database manually, you need to edit and run the scripts that come with WebSphere Process Server. This topic tells you how to edit and run scripts associated with DB2 for i5/OS and DB2 for IBM i databases.

About this task

Before you can run scripts to create a DB2 for i5/OS or DB2 for IBM i database manually, you need to customize them for WebSphere Process Server. WebSphere Process Server comes with following scripts:

Table 18. DB2 for i5/OS or DB2 for IBM i scripts for WebSphere Process Server

createDatabase_CommonDB.sql
createTable_RelationshipService.sql
dropTable_AppScheduler.sql
configCommonDB
createTable_CommonDB.sql
createTable_Recovery.sql
createTable_EsbLoggerMediation.sql
insertTable_CommonDB.sql
createDBTables
createTable_lockmanager.sql
createTable_customization.sql
createTable_mediation.sql
createTable_DirectDeploy.sql
createTable_AppScheduler.sql

Procedure

1. Make sure that you are using a user ID with sufficient authority to update the database schema.
2. Locate the directory where the database scripts are located:
   - *<media_root>*/dbscripts/CommonDB or *<extract_directory>*/dbscripts/CommonDB
3. Locate the configCommonDB file.
   a. Replace the *DB_NAME* variable with the database name, for example *LOCAL or *SYSBAS.
   b. Replace the *USER_NAME* variable with the DB2 for i5/OS or DB2 for IBM i user name, for example db2admin.
   c. Replace the *DB_SCHEMA* variable with the DB2 for i5/OS or DB2 for IBM i schema name, for example WPRCSDB.

   Important: You need to pass the **createDB** parameter to the configCommonDB script if you want to create a new local database; otherwise an existing database will be used.

   Also, you need to specify a unique schema name that does not exist on the system already.
4. Run the configCommonDB script in QShell. This in turn will run the createDBTables script to create the necessary schema and tables for the Common database.

   You must pass the **createDB** parameter to the configCommonDB script if you want to create a new local database; otherwise an existing database will be used. For example:

```
configCommonDB.sh createDB - create tables in a new database
```
```
configCommonDB.sh - create tables using an existing database
```

Important: You need to have `*SECOFR` authority on the IBM i system before you can run these scripts.

5. If there are any errors, or failure is indicated in your database client output, fix the reported errors and try again.

Results

The schema for the Common database is created.

Creating the DB2 database

In order to create a Common database manually, you need to edit and run the scripts that come with WebSphere Process Server. This topic tells you how to edit and run scripts associated with the DB2 database.

About this task

Before you can run scripts to create a DB2 database manually, you need to customize them for WebSphere Process Server. WebSphere Process Server comes with following scripts:

Table 19. DB2 scripts for WebSphere Process Server

configCommonDB.bat
configCommonDB.sh
createDBTables.bat
createDBTables.sh
createTable_CommonDB.sql
createTable_lockmanager.sql
createTable_Recovery.sql
createTable_EsbLoggerMediation.sql
createTable_governancerepository.sql
insertTable_CommonDB.sql
createTable_Relationship.sql
createTable_RelationshipService.sql
createTable_customization.sql
createTable_mediation.sql
createTable_DirectDeploy.sql
createTable_AppScheduler.sql

Procedure

1. Make sure that you are using a user ID with sufficient authority to update the database schema.
2. Locate the directory where the database scripts are located:
   - **Linux** **UNIX** `<media_root>`/dbscripts/CommonDB or `<extract_directory>`/dbscripts/CommonDB

- Windows `<media_root>\dbscripts\CommonDB` or `<extract_directory>\dbscripts\CommonDB`

3. Locate the `configCommonDB.bat` or `configCommonDB.sh` file and perform the following subtasks:

   a. Replace the *DB_NAME* variable with the database name, for example `WPRCSDB`.

   b. Replace the *USER_NAME* variable with the database user name, for example `db2admin`.

   You must pass the **createDB** parameter to the `configCommonDB` script if you want to create a new local database; otherwise an existing database will be used. For example:

   `configCommonDB.sh createDB` - create tables in a new database

   `configCommonDB.sh` - create tables using an existing database

   Important: You need to have `*SECOFR` authority on the IBM i system before you can run these scripts.

4. Locate the `createDatabase_CommonDB.sql` file and perform the following subtask.

   a. Replace the *DB_NAME* variable with the database name, for example `WPRCSDB`.

5. Run the `configCommonDB.bat` or `configCommonDB.sh` script. This in turn will run the `createDBTables.bat` or `createDBTables.sh` script to create the necessary schema and tables for the Common database.

6. If there are any errors, or failure is indicated in your database client output, fix the reported errors and try again.

Results

The DB2 database is created.

Creating the DB2 database for z/OS

In order to create a Common database manually, you need to edit and run the scripts that come with WebSphere Process Server. This topic tells you how to edit and run scripts associated with the DB2 for z/OS database.

About this task

Before you can run scripts to create a DB2 for z/OS database manually, you need to customize them for WebSphere Process Server. WebSphere Process Server comes with following scripts:

Table 20. DB2 for z/OS scripts for WebSphere Process Server

createTable_AppScheduler.sql
createTable_CommonDB.sql
createTable_DirectDeploy.sql
createTable_EsbLoggerMediation.sql
createTable_Recovery.sql
createTable_Relationship.sql
createTable_RelationshipService.sql
createTable_customization.sql

Table 20. DB2 for z/OS scripts for WebSphere Process Server (continued)

createTable_governancerepository.sql
createTable_lockmanager.sql
createTable_mediation.sql
insertTable_CommonDB.sql

Procedure

1. Make sure that you are using a user ID with sufficient authority to update the database schema.
2. Locate the directory where the database scripts are located:
   - **Linux**   **UNIX**   *<media_root>*/dbscripts/CommonDB or *<extract_directory>*/dbscripts/CommonDB
   - **Windows**   *<media_root>*\dbscripts\CommonDB or *<extract_directory>*\dbscripts\CommonDB
3. Choose whether to edit the scripts in directory DB2zOSV8 or DB2zOSV9.
4. Replace the following variables in the DB2 for z/OS scripts with your database-specific information: @DB_NAME@, @STOGRP@, and @SCHEMA@.
5. Run the DB2 for z/OS scripts, which are listed in Table 20 on page 35. For information about how to run a .sql script with your database, refer to the documentation for your database product.
6. If there are any errors, or failure is indicated in your database client output, fix the reported errors and try again.

Results

The DB2 for z/OS database is created.

Example

The createTable_lockmanager.sql script is missing from under the dbscripts/CommonDB/DB2zOSV8 folder in the WebSphere Enterprise Service Bus V7.0 CD image.

You can use the scripts from the CD image directly to set up their databases and not necessarily wait to install the entire product and, or create profiles to get a hold of these scripts.

If you use the scripts from the CD image to create the Common Database, you will miss the createTable_lockmanager.sql script which may cause runtime issues with response to these tables.

However, this file does show up after WebSphere Process Server is installed, under the <INSTALL>/dbscripts/CommonDB/DB2zOSV8 and also after a profile is created (under the profiles/<profiles>/dbscripts folder)

To fix this, install the product and then use the scripts from under the <INSTALL>/dbscripts/CommonDB/DB2zOSV8 location.

Creating the Informix database

In order to create a Common database manually, you need to edit and run the scripts that come with WebSphere Process Server. This topic tells you how to edit and run scripts associated with the Informix database.

About this task

Before you can run scripts to create an Informix database manually, you need to customize them for WebSphere Process Server. WebSphere Process Server comes with following scripts:

Table 21. Informix scripts for WebSphere Process Server

createDatabase_CommonDB.sql
createTable_RelationshipService.sql
dropTable_AppScheduler.sql
createTable_CommonDB.sql
createTable_lockmanager.sql
createTable_Recovery.sql
createTable_EsbLoggerMediation.sql
insertTable_CommonDB.sql
configCommonDB.bat
createTable_customization.sql
createTable_mediation.sql
createTable_DirectDeploy.sql
createTable_AppScheduler.sql

Procedure

1. Make sure that you are using a user ID with sufficient authority to update the database schema.
2. Locate the directory where the database scripts are located:
   - `Linux` `UNIX` *<media_root>*/dbscripts/CommonDB or *<extract_directory>*/dbscripts/CommonDB
   - `Windows` *<media_root>*\dbscripts\CommonDB or *<extract_directory>*\dbscripts\CommonDB
3. Locate the `createDatabase_CommonDB.sql` file and perform the following subtasks.
   a. Replace the *DB_NAME* variable with the name of the database, for example `WPRCSDB`.
   b. Replace the *DB_INSTANCE* variable with the Informix instance, for example `ol_myinstance`.
   c. Replace the *DB_LOCATION* variable with the Informix database location, for example `c:\informix`.
4. Run the `configCommonDB.bat` script. This in turn will run the `createDBTables` script to create the necessary schema and tables for the Common database.
5. If there are any errors, or failure is indicated in your database client output, fix the reported errors and try again.

Results

The Informix database is created.

Creating the Oracle database

In order to create a Common database manually, you need to edit and run the scripts that come with the WebSphere Process Server. This topic tells you how to edit and run scripts associated with the Oracle database.

About this task

Before you can run scripts to create an Oracle database manually, you need to customize them for WebSphere Process Server. WebSphere Process Server comes with following scripts:

Table 22. Oracle scripts for WebSphere Process Server

configCommonDB.bat
configCommonDB.sh
createDatabase_commonDB.sql
createTable_commonDB.sql
createTable_EsbLoggerMediation.sql
createTable_governancerepository.sql
createTable_lockmanager.sql
createTable_Recovery.sql
createTable_RelationshipMetadataTable.sql
insertTable_CommonDB.sql
createTable_RelationshipViewMetaaTable.sql
createTable_customization.sql
createTable_mediation.sql
createTable_DirectDeploy.sql
createTable_AppScheduler.sql

Procedure

1. Make sure that you are using a user ID with sufficient authority to update the database schema.
2. Locate the directory where the database scripts are located:
   - `Linux` `UNIX` *media_root*/dbscripts/CommonDB/oracle or *<extract_directory>*/dbscripts/CommonDB/oracle
   - `Windows` *media_root*\dbscripts\CommonDB\oracle or *<extract_directory>*\dbscripts\CommonDB\oracle
3. Locate the configCommonDB.bat or configCommonDB.sh file and perform following subtasks:
   a. Replace the *DB_NAME* variable with the Oracle Database name [SID], for example ORCL.
   b. Replace the *DB_USER* variable with Oracle user, for example orcCOMM.
4. Locate the createSchema_CommonDB.sql file which is a template used to create required schemas. To create a database schema:

a. Replace the *DB_USER* variable with the database schema name. For example, `orcCOMM`.

b. Replace the *dbCommonPassword* variable with the database schema password. For example, `youNameIt`. If not changed, you will be requested to enter a password for the *DB_USER*.

c. Repeat the above steps for each additional schema.

d. Required: Run the `createSchema_CommonDB.sql` script.

The following components require a schema. These schemas will be generated automatically if not passed during profile creation. The default schemas are:

Table 23. Default schemas

Component	Default value
CommonDB	*first3CharOfSID*COMM
Business Space	IBMBUSSP
SCA.SYSTEM ME	*first3CharOfSID*SS00
SCA.APP ME	*first3CharOfSID*SA00
CEI ME	*first3CharOfSID*CM00
BPC ME	*first3CharOfSID*BM00
CEI	*first3CharOfSID*CEID

For the above parameters, the value of the password depends on how you configure the profile. The Value can be a dbPassword or the value that is used while running the manageprofiles command-line utility. To run these scripts you must have SYSDBA privileges.

5. Copy all of the scripts from the *extract_directory*`\dbscripts\CommonDB` directory to the Oracle workstation and run the `configCommonDB.bat` or `configCommonDB.sh` script.

Note: Confirm that the database schema name that was specified in step 4 on page 38 above, for example, `orcCOMM`, is created before running this script because it uses the database schema name to connect the database for creating tables.

6. If there are any errors, or failure is indicated in your database client output, fix the reported errors and try again.

Results

The Oracle database is created.

Creating the Microsoft SQL Server database

In order to create a Common database manually, you need to edit and run the scripts that come with WebSphere Process Server. This topic tells you how to edit and run scripts associated with the Microsoft SQL Server database.

About this task

Before you can run scripts to create a Microsoft SQL Server database manually, you need to customize them for WebSphere Process Server. WebSphere Process Server comes with following scripts:

Table 24. Microsoft SQL Server scripts for WebSphere Process Server

createDatabase_CommonDB.sql
createTable_RelationshipService.sql
dropTable_AppScheduler.sql
createTable_CommonDB.sql
createTable_lockmanager.sql
createTable_Recovery.sql
createTable_EsbLoggerMediation.sql
insertTable_CommonDB.sql
configCommonDB.bat
createTable_customization.sql
createTable_mediation.sql
createTable_DirectDeploy.sql
createTable_AppScheduler.sql

Procedure

1. Make sure that you are using a user ID with sufficient authority to update the database schema.

2. Locate the directory where the database scripts are located:

   - `Linux` `UNIX` *<media_root>*/dbscripts/CommonDB or *<extract_directory>*/dbscripts/CommonDB

   - `Windows` *<media_root>*\dbscripts\CommonDB or *<extract_directory>*\dbscripts\CommonDB

3. Locate the `configCommonDB.bat` or `configCommonDB.sh` file and perform the following subtasks:

   a. Replace the *DB_NAME* variable with the database name, for example `WPRCSDB`.

   b. Replace the *DB_USER* variable with the database user name, for example `sqluser`.

   c. Replace the *DB_HOSTNAME* variable with the SQL host name, for example `me.usca.ibm.com`.

4. Run the Microsoft SQL Server scripts, which are listed in Table 24. For information on how to run a .sql script with your database, refer to the documentation for your database product.

5. If there are any errors, or failure is indicated in your database client output, fix the reported errors and try again.

Results

The Microsoft SQL Server database is created.

Installing the software

You can obtain WebSphere Process Server product files in two ways, from the disks in the product package or by downloading installation images from the Passport Advantage site, if you are licensed to do so. You install the software interactively from the launchpad program or silently by running Installation Manager in silent installation mode. In silent mode, the installation wizard does not display a graphical interface, but reads your responses from a response file.

Before installing the software for WebSphere Process Server, assess your current environment and your business requirements to ensure that the system you implement meets your needs. Middleware, such as WebSphere Process Server, requires that you evaluate many aspects of your enterprise information system (EIS), such as capacity and security.

For information about the images available for download, see the Passport Advantage Web site at http://www-01.ibm.com/software/lotus/passportadvantage/.

For more information about planning your installation and on the databases required by WebSphere Process Server, see the topics under Planning for WebSphere Process Server.

Then review installation prerequisites in "Prerequisites for installing WebSphere Process Server" on page 29.

After planning your installation and reviewing prerequisites, install the software from the appropriate disk or distribution media. You can choose to install the software interactively from the launchpad or in silent mode, using a response file to input the commands that are required to install the product package.

- To install interactively on all platforms, see "Installing WebSphere Process Server interactively for the first time" on page 43.
- Linux   UNIX   Windows   To install silently on Linux, UNIX, and Windows platforms, see "Silently installing WebSphere Process Server" on page 53.

  Note: HP-UX   Solaris   If you are installing on an HP-UX PA-RISC or Solaris on AMD 64-bit platform, you must use the silent installation mode.

The maximum recommended path length on the Windows 2000, Windows XP, Windows Vista, and Windows 7 operating systems is 60 characters.

Installing the software creates a set of core product files on the workstation. These files are needed for you to configure stand-alone servers and deployment environments.

After performing the installation, you can create a stand-alone server, a deployment manager, a custom profile, or a deployment environment configuration using the Profile Management Tool. You can also use the First steps console to validate that a stand-alone server or deployment manager profile was created successfully, to start and stop the server, and to perform other tasks.

Starting the launchpad

The launchpad for WebSphere Process Server is the single point of reference for installing the entire server environment, which can include WebSphere Process Server, WebSphere Application Server Network Deployment, a Web server, and additional supporting software and documentation.

Before you begin

The launchpad application is available on the product DVD and on downloaded installation images. You must satisfy the following prerequisites before starting it:

- Review the list of prerequisites for installing the product in the topic "Prerequisites for installing WebSphere Process Server" on page 29.
- Because the launchpad is a Web application, ensure that you have a supported version of a Web browser installed.

  `Linux` `UNIX` `Windows` The platform-specific topics under Preparing the operating system for installation in the WebSphere Application Server Network Deployment information center contain detailed instructions for installing supported Web browsers on all platforms.

Procedure

1. Log on to the system.
2. Access the media in one of the following ways, depending on whether you are installing from the product DVD or from images downloaded from Passport Advantage.

   - If you are installing from the product DVD, perform the following steps:

     a. Insert the product disk labeled *WebSphere Process Server Version 7.0* into the disk drive. Mount the disk drive if necessary. If autorun is enabled on your workstation, the WebSphere Process Server launchpad program automatically opens.

        If autorun is not enabled: If autorun is not enabled on your workstation, enter one of the following commands to start the launchpad manually:

        - `Linux` `UNIX` *mount_point*/launchpad.sh

        - `Windows` (from a command line) *DVD_root*\launchpad.exe

   - If you are installing from images downloaded from Passport Advantage, perform the following steps:

     a. Navigate to the directory into which you extracted the images.

     b. Enter one of the following commands to start the launchpad:

        - `Linux` `UNIX` *extract_directory*/launchpad.sh

        - `Windows` (from a command line) *extract_directory*\launchpad.exe

Results

The launchpad opens. If you have a problem starting the launchpad, use the troubleshooting information in "Troubleshooting the launchpad application or First Steps" on page 146 to correct the problem. If the launchpad did not initialize in the language used on your system, select your language in the **Select a language** field.

You can use the launchpad to start the installation of WebSphere Process Server and related products.

What to do next

Return to the installation procedure from which you accessed this topic to continue.

Installing WebSphere Process Server interactively for the first time

You can install WebSphere Process Server interactively. This procedure assumes that you are starting the installation process from the launchpad application. It also assumes that you do not have existing installations of the prerequisite base products necessary for WebSphere Process Server installation. These include WebSphere Application Server Network Deployment, WebSphere Application Server Feature Pack for XML, and WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature.

Before you begin

Before you can install WebSphere Process Server, perform the following tasks:

- Review the list of prerequisites for installing the product in the topic "Prerequisites for installing WebSphere Process Server" on page 29. Of particular importance are operating system and software prerequisite levels. Although the installation process automatically checks for prerequisite operating system patches, review the prerequisites at http://www.ibm.com/support/docview.wss?uid=swg27006205 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. It also lists the required levels of all prerequisite software.
- Review the "Default installation directories for the product and profiles" on page 127 information to confirm the installation locations for Installation Manager and WebSphere Application Server.
- Because the launchpad is a Web application, ensure that you have a supported version of a Web browser installed.

  `Linux`   `UNIX`   `Windows` The platform-specific topics under Preparing the operating system for installation in the WebSphere Application Server Network Deployment information center contain detailed instructions for installing supported Web browsers on all platforms.

About this task

When you start the installation process using the launchpad application and are installing the product together with a new installation of WebSphere Application Server Network Deployment, the launchpad installs IBM Installation Manager (if it is not already installed), WebSphere Application Server Network Deployment, WebSphere Application Server Feature Pack for XML, WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature, and WebSphere Process Server.

Important: During product installation or modification, you might see errors in the Installation Manager interface or log files similar to the following:

```
228 ERROR  07:41.26 Installation Manager cannot remove feature import.configLauncher.
feature from an installation package that was imported to Installation Manager.
229 ERROR  07:41.54 Installation Manager cannot remove feature import.productProviders.
feature from an installation package that was imported to Installation Manager.
```

You can safely ignore such errors.

Procedure

1. Start the launchpad application by navigating into the directory where you extracted the image and entering the following command:

   - [Linux] [UNIX] **On Linux and UNIX platforms:** *extract_directory*/launchpad.sh

   - [Windows] **On Windows platforms (from a command line):** *extract_directory*\launchpad.exe

2. In the left pane of the launchpad, click one of the following entries depending on whether you are a root/Administrator or nonroot/nonadministrative user:

   - If you are a root or an Administrator user, click **New installation**.
   - If you are a nonroot or a nonadministrative user, click **Nonadministrative or nonroot installation**.

3. If you already have IBM Installation Manager installed, ensure that it is *not* running.

4. In the right pane of the launchpad, in step 1, specify the location for the WebSphere Application Server Network Deployment installation, or accept the default location, and click **Install WebSphere Application Server**.

   Restrictions:

   - [Windows] **On Windows platforms:** IBM Installation Manager requires that its installation directory path be 80 characters or less. Thus, it is strongly recommended that you keep your user ID to 20 characters or less.

   - If you specify your own directory for the WebSphere Application Server Network Deployment installation, that directory cannot exist, even if empty.

   The launchpad application performs the following tasks:

   - Installs WebSphere Application Server Network Deployment into the directory you specify.

   - Installs IBM Installation Manager to its default installation location, if it is not already installed. If IBM Installation Manager is not at the required level, the launchpad application updates it to the correct level.

     Review the "Default installation directories for the product and profiles" on page 127 information to confirm the installation locations for Installation Manager and WebSphere Application Server.

     You can review additional Installation Manager documentation in the Installation Manager Information Center.

   - Imports WebSphere Application Server into Installation Manager automatically.

   Important: This process occurs silently and can take several minutes. Do *not* proceed until a message indicates a successful installation and import into Installation Manager. Instead of a success message, you might receive one of the following messages:

   - `WebSphere Application Server installation failed.` In this case, review the following log file to identify the cause:

     - [Linux] [UNIX] **On Linux and UNIX platforms:** *was_home*/logs/install/log.txt

     - [Windows] **On Windows platforms:** *was_home*\logs\install\log.txt

If the `logs` directory does not exist on your system, the installation failed very early in the process. In this case, review the following log file:

  – `Linux` `UNIX` **On Linux and UNIX platforms:** *user_home*/waslogs/log.txt

  – `Windows` **On Windows platforms:** *user_home*\waslogs\log.txt

- `WebSphere Application Server installation was successful,` but there were errors importing into Installation Manager. In this case, review the following log file to identify the cause:

  – `Linux` `UNIX` **On Linux and UNIX platforms:** *was_home*/logs/launchpad_import.txt

  – `Windows` **On Windows platforms:** *was_home*\logs\launchpad_import.txt

5. In the right pane of the launchpad, in step 2, click **Install WebSphere Process Server**. The launchpad application starts Installation Manager and its Install Packages wizard.

6. On the Install page of the Install Packages wizard, all recommended packages, including WebSphere Application Server Feature Pack for XML, WebSphere Application Server Feature Pack for Service Component Architecture (SCA), and WebSphere Process Server are preselected for installation. Click **Next**.

7. On the Install Packages wizard Licenses page, read through the license agreements and then select **I accept the terms in the license agreements**. Click **Next**. The licenses for the feature packs are also displayed in the panel. You accept for all the licenses.

8. On the Install Packages wizard Location page, **IBM WebSphere Application Server - ND_xxxxx** (where **xxxxx** is the date timestamp) and the **Use the existing package group** radio button are selected by default. Leave those selections as they are and click **Next**.

   Note: The Install Packages wizard displays a message if it detects any running processes. If you see this message, click **Cancel**, shut down the running processes, and begin the installation again.

9. The Install Packages wizard checks your operating system to make sure that it meets the prerequisites for installing WebSphere Process Server. The action you take depends on the results of the prerequisite check:

   - If the prerequisite check is successful (that is, a supported operating system is found), no message is displayed. The installation continues on to the Install Packages wizard Features page. Proceed to step 10.

   - If the prerequisite check is not successful (for example, a supported operating system is not at the minimum supported level), you see an error message and the installation stops. You must address the problem described in the message before you can install WebSphere Process Server.

   - 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 a warning. You can continue with the installation, but the installation or product operation might not succeed until you apply maintenance.

     If you see such a warning, go to the product support Web pages and 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.

10. On the Install Packages wizard Features page, accept the default selections and click **Next**.

a. Optional: To install samples, expand **IBM WebSphere Process Server 7.0.0.0** and then **WebSphere Process Server**, and select the check box for **Sample applications**. If you choose not to install sample applications, you can install them later by following the instructions under "To install the samples or a default stand-alone development profile after installation".

b. Optional: To install a default stand-alone development profile for WebSphere Process Server, expand **IBM WebSphere Process Server 7.0.0.0** and then **WebSphere Process Server**, and select the check box for **Stand-alone development WebSphere Process Server profile (qwps)**. To install a default stand-alone development profile for WebSphere Enterprise Service Bus, select the check box for **Stand-alone development WebSphere Enterprise Service Bus profile (qesb)**.

The stand-alone development profile is a default development profile that comes with Business Rules Manager enabled. If you select to create a development profile, you are asked to supply your administrator security ID and password credentials. You cannot use a development profile in a production environment. If you choose not to install a default stand-alone development profile, you can install one later by following the instructions under "To install the samples or a default stand-alone development profile after installation".

11. Review the summary information. If the summary information is incorrect, click **Back** to change your selections.

12. Click **Install**. When the installation is complete, a page displays the status of the installation and which packages have been successfully installed.

   Important: This process can take several minutes. Do *not* proceed until this page appears.

13. To launch the Profile Management Tool, leave the **Profile Management Tool** radio button selected. Otherwise, select the radio button for **None**.

14. Click **Finish**.

15. Close Installation Manager if needed.

Results

WebSphere Process Server is installed.

What to do next

You must define a stand-alone server profile or a deployment manager in the Profile Management Tool or using the manageprofiles command-line utility. Only profiles created with the Profile Management Tool or manageprofiles command-line utility can be used in production. See the topics under "Creating profiles" on page 196 and "Augmenting profiles" on page 300 for more information.

Restriction:

If you created a stand-alone development profile during installation, remember that it does not work in a production environment. It is intended to help you gain familiarity with WebSphere Process Server without having to create a working production profile. You can start it from its First steps console by performing the following steps:

1. Open a command window.

2. Change to one of the following directories depending on your platform and on which type of profile you created:

- `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/`profiles/qwps/firststeps/wbi`

- `Windows` **On Windows platforms:** *install_root*\`profiles\qwps\firststeps\wbi`

- `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/`profiles/qesb/firststeps/esb`

- `Windows` **On Windows platforms:** *install_root*\`profiles\qesb\firststeps\esb`

3. Issue the firststeps command to start the console:

- `Linux` `UNIX` **On Linux and UNIX platforms:** `./firststeps.sh`

- `Windows` **On Windows platforms:** `firststeps.bat`

To install the samples or a default stand-alone development profile after installation:

If you chose not to install the samples or a default stand-alone development profile, you can do so later by performing the following steps:

1. Launch the Installation Manager manually. See "Starting IBM Installation Manager manually" on page 67 for instructions.

2. Click **File > Preferences**.

3. In the Repositories Preferences page, click **Add Repository**.

4. In the Add Repository page, browse to the location of the following file, ensure that the check box beside **Search service repositories during installation and updates** is *not* selected, and then click **OK**.

- `Linux` `UNIX` **On Linux and UNIX platforms:** *extract_directory*/`repository/repository.config`

- `Windows` **On Windows platforms (from a command line):** *extract_directory*\`repository\repository.config`

5. Return to the first page of the Installation Manager.

6. Select **Modify**.

7. Follow the instructions on the Modify wizard pages to install the sample applications, or to create a stand-alone WebSphere Process Server or WebSphere Enterprise Service Bus profile.

Installing WebSphere Process Server interactively over an existing installation of WebSphere Application Server Network Deployment

You can install WebSphere Process Server interactively over an existing installation of a supported version of WebSphere Application Server Network Deployment. This procedure assumes that you are starting the installation process from the launchpad application and that you are a root or administrator user. It also assumes that you have an existing installation of a supported version of WebSphere Application Server Network Deployment, and might or might not have existing installations of other prerequisite base products necessary for WebSphere Process Server installation, including WebSphere Application Server Feature Pack for XML and WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature.

Before you begin

Before you can install WebSphere Process Server, perform the following tasks:

- Review the list of prerequisites for installing the product in the topic "Prerequisites for installing WebSphere Process Server" on page 29. Of particular importance are operating system and software prerequisite levels. Although the installation process automatically checks for prerequisite operating system patches, review the prerequisites at http://www.ibm.com/support/docview.wss?uid=swg27006205 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. It also lists the required levels of all prerequisite software.
- Review the "Default installation directories for the product and profiles" on page 127 information to confirm the installation locations for Installation Manager and WebSphere Application Server.
- Because the launchpad is a Web application, ensure that you have a supported version of a Web browser installed.

   `Linux`   `UNIX`   `Windows` **On Linux, UNIX and Windows platforms:** The platform-specific topics under Preparing the operating system for installation in the WebSphere Application Server Network Deployment information center contain detailed instructions for installing supported Web browsers on all platforms.

About this task

When you install WebSphere Process Server over an existing installation of WebSphere Application Server Network Deployment, you must ensure that the installation is at a supported level and that necessary installation tooling is installed. The launchpad application guides you through this process.

Important: During product installation or modification, you might see errors in the Installation Manager interface or log files similar to the following:

```
228 ERROR  07:41.26 Installation Manager cannot remove feature import.configLauncher.
feature from an installation package that was imported to Installation Manager.
229 ERROR  07:41.54 Installation Manager cannot remove feature import.productProviders.
feature from an installation package that was imported to Installation Manager.
```

You can safely ignore such errors.

Procedure

1. Start the launchpad application by navigating into the directory where you extracted the image and entering the following command:

   - `Linux`   `UNIX` **On Linux and UNIX platforms:** *extract_directory*/`launchpad.sh`

   - `Windows` **On Windows platforms (from a command line):** *extract_directory*\`launchpad.exe`

2. In the left pane of the launchpad, click **Installation on existing WebSphere Application Server**.

3. Choose from the following actions based on whether you have IBM Installation Manager installed at the required level:

   - If you have Installation Manager installed at the required level or higher, go to step 4 on page 49.

- If you do not have Installation Manager installed, or if your installation is below the required level, perform the following steps:

  a. On the "Installation on existing WebSphere Application Server" page of the launchpad, in step 1, click **Install or update IBM Installation Manager**. The Installation Packages wizard opens in a separate window. IBM Installation Manager Version is preselected.

  b. Click **Next**.

  c. On subsequent pages of the Installation Manager, follow the instructions on each page, accepting the defaults. If Installation Manager is already installed on your system, the application checks that it is at the correct level and updates it to the correct level if necessary.

  d. Close the success page that appears after installing Installation Manager, but do *not* click **Restart Installation Manager**.

  e. Return to the launchpad application.

  You can review additional Installation Manager documentation in the Installation Manager Information Center.

4. Choose from the following actions based on the level of your installed version of WebSphere Application Server Network Deployment:

   - If your installation is at the required level of maintenance or higher, go to step 5.

   - If your installation is below the required level of maintenance, first, ensure that the Installation Manager application is closed. Then, on the "Installation on existing WebSphere Application Server" page of the launchpad, in step 2, click **Update WebSphere Application Server** to run the WebSphere Application Server common installation package. Perform the following steps:

     a. Navigate through the WebSphere Application Server installer to the page "Detected IBM WebSphere Application Server."

     b. Select **Apply maintenance or add features to an existing installation**, specifying the installation on which you are installing WebSphere Process Server.

        Important: If you want to install the WebSphere Process Server samples, the installation of WebSphere Application Server Network Deployment that you use must have samples installed.

     c. Continue through the remaining pages of the installer. The installer adds maintenance to your existing WebSphere Application Server installation.

5. Choose from the following actions based on whether you have already imported your installation of WebSphere Application Server Network Deployment into Installation Manager:

   - If you have already imported your installation *and its maintenance level has not changed*, go to step 6 on page 50.

   - If you have not already imported your installation or if you have already imported it and its maintenance level has changed, import it by performing the following steps:

     a. On the "Installation on existing WebSphere Application Server" page of the launchpad, in step 3, click **Import WebSphere Application Server into Installation Manager**. The launchpad starts the Installation Manager application.

     b. From the start page of the Installation Manager, click **Import**.

      c. On the Import Existing WebSphere Installation page, specify the location of the WebSphere Application Server Network Deployment on which you want to install WebSphere Process Server.

      d. Click **Next** and proceed through the subsequent pages, which set this directory location and the location of your shared resources directory.

      e. After the import process completes, on the success page, click **Finish**.

      f. Close Installation Manager.

6. Choose from the following actions based on whether you have already installed WebSphere Application Server Feature Pack for XML and/or WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with or without the Service Data Objects (SDO) feature on your installation of WebSphere Application Server Network Deployment:

   - If you do *not* have either feature pack installed, go to step 8.

   - If you have one or both feature packs installed, perform the following steps:

     a. On the "Installation on existing WebSphere Application Server" page of the launchpad, in step 4, click **Update feature packs**. The launchpad starts the Installation Manager application.

     b. From the Start page of the Installation Manager, click **Update**.

     c. Follow steps 5 on page 106 through 12 on page 106 in the procedure "Updating the software interactively" on page 105, selecting the package group **IBM WebSphere Application Server - ND**.

7. Choose from the following actions based on whether you have already installed the Service Data Objects (SDO) feature on your installation of WebSphere Application Server Feature Pack for Service Component Architecture (SCA):

   - If you have already installed the feature, go to step 8.

   - If you have *not* already installed the feature, perform the following steps:

     a. Start Installation Manager. See "Starting IBM Installation Manager manually" on page 67 for more information.

     b. From the Start page of the Installation Manager, click **Modify**.

     c. Follow steps 4 on page 67 through 8 on page 67 in the procedure "Modifying a product installation" on page 66, selecting the package group that contains WebSphere Application Server Feature Pack for Service Component Architecture (SCA) and the SDO feature.

8. Ensure that the Installation Manager application is closed. Then, in step 5 on the "Installation on existing WebSphere Application Server" page of the launchpad, click **Install WebSphere Process Server**. The launchpad application starts Installation Manager and its Install Packages wizard.

9. On the Install page of the Install Packages wizard, all recommended packages, including WebSphere Application Server Feature Pack for XML, WebSphere Application Server Feature Pack for Service Component Architecture (SCA), and WebSphere Process Server are preselected for installation. Click **Next**.

   Important: Clear the check box beside any feature pack you have already installed.

10. On the Install Packages wizard Licenses page, read through the license agreements and then select **I accept the terms in the license agreements**. Click **Next**. The licenses for the feature packs are also displayed in the panel. You accept for all the licenses.

11. On the Install Packages wizard Location page, select the package group for your installation of WebSphere Application Server and click **Next**.

Note: The Install Packages wizard displays a message if it detects any running processes. If you see this message, click **Cancel**, shut down the running processes, and begin the installation again.

12. The Install Packages wizard checks your operating system to make sure that it meets the prerequisites for installing WebSphere Process Server. The action you take depends on the results of the prerequisite check:

    - If the prerequisite check is successful (that is, a supported operating system is found), no message is displayed. The installation continues on to the Install Packages wizard Features page. Proceed to step 13.

    - If the prerequisite check is not successful (for example, a supported operating system is not at the minimum supported level), you see an error message and the installation stops. You must address the problem described in the message before you can install WebSphere Process Server.

    - 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 a warning. You can continue with the installation, but the installation or product operation might not succeed until you apply maintenance.

      If you see such a warning, go to the product support Web pages and 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.

13. On the Install Packages wizard Features page, accept the default selections and click **Next**.

    a. Optional: To install samples, expand **IBM WebSphere Process Server 7.0.0.0** and then **WebSphere Process Server**, and select the check box for **Sample applications**. To install samples for WebSphere Process Server, you must have WebSphere Application Server samples installed. If you choose not to install sample applications, you can install them later by following the instructions under "To install the samples or a default stand-alone development profile after installation".

    b. Optional: To install a default stand-alone development profile for WebSphere Process Server, expand **IBM WebSphere Process Server 7.0.0.0** and then **WebSphere Process Server**, and select the check box for **Stand-alone development WebSphere Process Server profile (qwps)**. To install a default stand-alone development profile for WebSphere Enterprise Service Bus, select the check box for **Stand-alone development WebSphere Enterprise Service Bus profile (qesb)**.

      The stand-alone development profile is a default development profile that comes with Business Rules Manager enabled. If you select to create a development profile, you are asked to supply your administrator security ID and password credentials. You cannot use a development profile in a production environment. If you choose not to install a default stand-alone development profile, you can install one later by following the instructions under "To install the samples or a default stand-alone development profile after installation".

14. Review the summary information. If the summary information is incorrect, click **Back** to change your selections.

15. Click **Install**. When the installation is complete, a page displays the status of the installation and which packages have been successfully installed.

    Important: This process can take several minutes. Do *not* proceed until this page appears.

16. To launch the Profile Management Tool, leave the **Profile Management Tool** radio button selected. Otherwise, select the radio button for **None**.

17. Click **Finish**.

18. Close Installation Manager if needed.

Results

WebSphere Process Server is installed.

What to do next

You must define a stand-alone server profile or a deployment manager in the Profile Management Tool or using the manageprofiles command-line utility. Only profiles created with the Profile Management Tool or manageprofiles command-line utility can be used in production. See the topics under "Creating profiles" on page 196 and "Augmenting profiles" on page 300 for more information.

Restriction:

If you created a stand-alone development profile during installation, remember that it does not work in a production environment. It is intended to help you gain familiarity with WebSphere Process Server without having to create a working production profile. You can start it from its First steps console by performing the following steps:

1. Open a command window.

2. Change to one of the following directories depending on your platform and on which type of profile you created:

    - ▮ Linux ▮ UNIX **On Linux and UNIX platforms:** *install_root*/`profiles/qwps/firststeps/wbi`

    - ▮ Windows **On Windows platforms:** *install_root*\`profiles\qwps\firststeps\wbi`

    - ▮ Linux ▮ UNIX **On Linux and UNIX platforms:** *install_root*/`profiles/qesb/firststeps/esb`

    - ▮ Windows **On Windows platforms:** *install_root*\`profiles\qesb\firststeps\esb`

3. Issue the firststeps command to start the console:

    - ▮ Linux ▮ UNIX **On Linux and UNIX platforms:** `./firststeps.sh`

    - ▮ Windows **On Windows platforms:** `firststeps.bat`

To install the samples or a default stand-alone development profile after installation: If you chose not to install the samples or a default stand-alone development profile, you can do so later by performing the following steps:

1. Launch the Installation Manager manually. See "Starting IBM Installation Manager manually" on page 67 for instructions.

2. Click **File > Preferences**.

3. In the Repositories Preferences page, click **Add Repository**.

4. In the Add Repository page, browse to the location of the following file, ensure that the check box beside **Search service repositories during installation and updates** is *not* selected, and then click **OK**.

- ▪ `Linux` `UNIX` **On Linux and UNIX platforms:** *extract_directory*/repository/repository.config
- ▪ `Windows` **On Windows platforms (from a command line):** *extract_directory*\repository\repository.config

5. Return to the first page of the Installation Manager.
6. Select **Modify**.
7. Follow the instructions on the Modify wizard pages to install the sample applications, or to create a stand-alone WebSphere Process Server or WebSphere Enterprise Service Bus profile.

Silently installing WebSphere Process Server

You can install the WebSphere Process Server product package in silent installation mode. When you install in silent mode, the user interface is not available. Instead, you use a response file to input the commands that are required to install the product package. This procedure assumes that you might or might not have existing installations of the prerequisite base products necessary for WebSphere Process Server installation. These prerequisite products include WebSphere Application Server Network Deployment, Installation Manager, WebSphere Application Server Feature Pack for XML, and WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature.

Before you begin

Before you can install WebSphere Process Server, you must review the list of prerequisites for installing the product in the topic "Prerequisites for installing WebSphere Process Server" on page 29.

Of particular importance are operating system and software prerequisite levels. Although the installation process automatically checks for prerequisite operating system patches, review the prerequisites at http://www.ibm.com/support/docview.wss?uid=swg27006205 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. It also lists the required levels of all prerequisite software.

Review the "Default installation directories for the product and profiles" on page 127 information to confirm the installation locations for Installation Manager and WebSphere Application Server.

About this task

You start the installation process by running the run_templates or run_template.bat script, which you edit. The script performs some or all the following tasks:
- Installs WebSphere Application Server Network Deployment.
- Installs IBM Installation Manager if it is not already installed or updates it to the appropriate level if it is.
- Imports WebSphere Application Server Network Deployment into Installation Manager.
- Installs the required base products and WebSphere Process Server using a response file that you create.

- Automatically configures the installation with the location of the repository that contains the product packages.

Important: During product installation or modification, you might see errors in the Installation Manager interface or log files similar to the following:

```
228 ERROR  07:41.26 Installation Manager cannot remove feature import.configLauncher.
feature from an installation package that was imported to Installation Manager.
229 ERROR  07:41.54 Installation Manager cannot remove feature import.productProviders.
feature from an installation package that was imported to Installation Manager.
```

You can safely ignore such errors.

Procedure

1. Locate the default response file that you will use to install the required base products and WebSphere Process Server.

   The response file name and directory are listed here:

   - **Linux** **UNIX** *DVD_root* or *extract_root*/responsefiles/wbi/ template_response.xml

   - **Windows** *DVD_root* or *extract_root*\responsefiles\wbi\ template_response.xml

2. Edit the response file. Modify parameters as directed in the text of the response file template. You can create a response file by recording your actions in Installation Manager. When you record a response file, the selections that you make in Installation Manager are stored in an XML file. When you run Installation Manager in silent mode, Installation Manager uses the data in the XML response file to perform the installation. Refer to http:// publib.boulder.ibm.com/infocenter/install/v1r2/index.jsp?topic=/ com.ibm.silentinstall12.doc/topics/t_silent_create_response_files_IM.html for more information.

3. The script file is located in the same directory as the response file:

   - **Linux** **UNIX** *DVD_root* or *extract_root*/responsefiles/wbi/ run_templates

   - **Windows** *DVD_root* or *extract_root*\responsefiles\wbi\run_template.bat

4. Edit the script, modifying parameters as directed in the text of the script. Comment out any parameters not needed for your installation. For example, comment out the parameter to install WebSphere Application Server Network Deployment if you already have it installed on your system and intend to install WebSphere Process Server on top of it.

   Note: If running the run_templates script as a non-root user, use the following command in the script to install the IBM Installation Manager. For more information, refer to "Silently installing WebSphere Process Server as a non-root user" on page 55.

   ```
   "${IM_IMAGE}"/userinst  --launcher.ini
   "${IM_IMAGE}"/user-silent-install.ini -input
   "${PROGDIR}"/template_response.xml -log
   ${WAS_LOCATION}"/wps/silent_install.log
   ```

5. Run the run_templates script.

Results

The run_templates script reads the response file, installs any required prerequisites and WebSphere Process Server, and writes a log file to the directory you specified.

See "Installation and profile creation log files" on page 145.

What to do next

You must define a stand-alone server profile or a deployment manager in the Profile Management Tool or using the manageprofiles command-line utility. Only profiles created with the Profile Management Tool or manageprofiles command-line utility can be used in production. See "Creating profiles" on page 196 and "Augmenting profiles" on page 300 for more information.

Silently installing WebSphere Process Server as a non-root user

You can install the WebSphere Process Server product package in silent installation mode as a non-root user. When you install in silent mode, the user interface is not available. Instead, you use a response file to input the commands that are required to install the product package. This procedure assumes that you might or might not have existing installations of the prerequisite base products necessary for WebSphere Process Server installation. These prerequisite products include WebSphere Application Server Network Deployment, Installation Manager, WebSphere Application Server Feature Pack for XML, and WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature.

Before you begin

Before you can install WebSphere Process Server, you must review the list of prerequisites for installing the product in the topic "Prerequisites for installing WebSphere Process Server" on page 29.

About this task

You start the installation process by running the run_templates or run_template.bat script, which you edit. The script performs some or all the following tasks:

- Installs WebSphere Application Server Network Deployment.
- Installs IBM Installation Manager if it is not already installed or updates it to the appropriate level if it is.
- Imports WebSphere Application Server Network Deployment into Installation Manager.
- Installs the required base products and WebSphere Process Server using a response file that you create.
- Automatically configures the installation with the location of the repository that contains the product packages.

Procedure

1. Download the appropriate product image for your operating system, and then extract the product image. For example, for a Solaris 64bit image, WPS_v7_Solaris_SPARC_64_Install.tar.gz:

```
mkdir <extract_root>
cd <extract_root>
gunzip -c WPS_v7_Solaris_SPARC_64_Install.tar.gz | tar xvf -
```

The response file and script that you will use to install WebSphere Process Server are located in the following location:extract_root/responsefiles/WBI

2. Back up the original run_templates script and `template_response.xml` response file. For example:

```
cp run_templates run_templates.org
cp template_response.xml my_response.xml file
```

3. Edit the run_templates script as follows:

   a. In the script, specify where you want to install WebSphere Application Server.

      Note: Assume WebSphere Application Server and IBM Installation Manager are installed under the following locations:

      WAS: `/export/home/wps/wpsv7/ProcServer`

      IBM IM: `/export/home/wps/wpsv7/IM/eclipse`
      For example:

      ```
      WAS_LOCATION=/export/home/wps/wpsv7/ProcServer
      ```

      ```
      Install command for WebSphere Application Server:
      ```

      ```
      "${WAS_IMAGE}"/install -silent -OPT silentInstallLicenseAcceptance=true
      -OPT allowNonRootSilentInstall=true -OPT disableOSPrereqChecking=true
      -OPT disableNonBlockingPrereqChecking=true -OPT installType=installNew
      -OPT profileType=none -OPT feature=samplesSelected -OPT
      feature=languagepack.console.all -OPT feature=languagepack.server.all
      -OPT installLocation="${WAS_LOCATION}"
      ```

      The example above installs WebSphere Application Server in the location specified by `WAS_LOCATION`, but does not create any profiles. You must complete the WebSphere Process Server installation and then create profiles as a post-installation task.

      If you have already installed WebSphere Application Server, edit the run_templates script to comment out the install command listed above.

   b. Change the command used for installing the IBM Installation Manager. Installation Manager installation can be done by both root and non-root user installs. The installation location can be defined in the `my_response.xml` file. Refer to Step 4a.

      If you are a non-root user, update the run_templates script with the following command to install Installation Manager:

      ```
      "${IM_IMAGE}"/userinst  --launcher.ini "${IM_IMAGE}"/user-silent-install.ini
      -input "${PROGDIR}"/my_response.xml -log "${WAS_LOCATION}"/logs/wps/silent_install.log
      ```

      If you are a root user, you can use the following command:

      ```
      "${IM_IMAGE}"/install  --launcher.ini "${IM_IMAGE}"/silent-install.ini
      -input "${PROGDIR}"/my_response.xml -log "${WAS_LOCATION}"/logs/wps/silent_install.log
      ```

   Note: Important notes on Installation Manager installation:

   - `WAS_LOCATION`/logs/wps/silent_install.log file used with -log option contains the results of all the actions in the response file. Review this log file to see the results.
   - If you install IBM IM as a non-root user, the `/var/ibm/InstallationManager` folder is created under the user's home directory `/home/user`/var/ibm/ `InstallationManager`. If you install as a root user, this folder is created directly under `/var/ibm/InstallationManager`. This is the Agent Data Location (more info) that holds information about Installation Manager and the different packages it handles. If you would prefer a different location for

this folder, you can use a **-dataLocation** parameter in the install action for Installation Manager in the run_templates script, as shown in the following example:

```
IM_IMAGE/install  --launcher.ini IM_IMAGE
/silent-install.ini -dataLocation <path_IBMIM_dataLocationFolder> -input
PROGDIR/my_response.xml -log WAS_LOCATION/logs/wps/silent_install.log
```

4. Edit the copy of the response file (for example, `my_response.xml`) as follows. This file contains all the responses to the install actions that install Installation Manager and WebSphere Process Server.

   a. Edit the Installation manager installation location.

   ```
   <!-- #########
   This profile node defines where IBM Installation Manager (IM) is/or
   will be installed. If you want to modify where IM is installed modify
   both the installLocation and eclipseLocation values to specify the correct directory
   ##########-->
   <profile kind='self' installLocation='/export/home/wps/wpsv7/IM/eclipse'
   id='IBM Installation Manager'> <data key='eclipseLocation'
   value='/export/home/wps/wpsv7/IM/eclipse'/></profile>
   <!-- #######
   Modify to change the location of the eclipseCache (only if no cache has
   been created yet). eclipseCache is the Shared Resources Directory.
   #########-->
   <preference value="/export/home/wps/wpsv7/IM/eclipseCache"
   name="com.ibm.cic.common.core.preferences.eclipseCache" />
   ```

   In the above example, the response file has been modified to specify that the Installation Manager should be installed in `/export/home/wps/wpsv7/IM/eclipse` and the cache should be installed in `/export/home/wps/wpsv7/IM/eclipseCache`.

   b. If you are a non-root user, you need to ensure you will have write access to the directory where you intend to do your installation.

   Note: References to `profile` in Installation Manager refers to the binary installation location, not the WebSphere Application Server profiles.

   ```
   <profile installLocation='/export/home/wps/wpsv7/ProcServer'
   id='IBM WebSphere Application Server - ND'><data key='eclipseLocation'
   value='/export/home/wps/wpsv7/ProcServer'/>
   ```

   The `id` field (IBM WebSphere Application Server - ND) is what identifies this particular WebSphere Application Server installation to Installation Manager. You can change this to anything you prefer, but make sure to use the same value further down in the response file while importing the WebSphere Application Server location and updating other packages.

   c. Specify that you want to import the WebSphere Application Server location. This command directs Installation Manager to import WebSphere Application Server Network Deployment, the location of which you specified in Step 4b. If you changed the profile ID above, you must also change the profile ID here.

   ```
   <import profile="IBM WebSphere Application Server - ND" type="WAS" />
   ```

   d. Specify that you want to install the required prerequisites and WebSphere Process Server. The following lines direct Installation Manager to install the IM-based offering. If you changed the profile ID above, you must also change the profile ID here. Note that profile in Installation Manager refers to the binary installation location.

   ```
   <install>
   <offering profile="IBM WebSphere Application Server - ND" id="com.ibm.websphere.XML.v10" />
   <offering profile="IBM WebSphere Application Server - ND" id="com.ibm.websphere.SCA.v10" />
   <offering profile="IBM WebSphere Application Server - ND" id="com.ibm.ws.WPS" />
   </install>
   ```

5. Run the run_templates script. For example, refer to the following run_templates script with console output, for a non-root user:

```
bash-3.00$ ./run_templates
/home/wpsuser/WPS70/responsefiles/WBI/../../WAS/install -silent -OPT
silentInstallLicenseAcceptance=true -OPT allowNonRootSilentInstall=true -
OPT disableOSPrereqChecking=true
-OPT disableNonBlockingPrereqChecking=true -OPT installType=installNew -
OPT profileType=none
-OPT feature=samplesSelected -OPT feature=languagepack.console.all -OPT
feature=languagepack.server.all -OPT installLocation=/export/home/wps/wpsv7/ProcServer
WAS rc: 0
/home/wpsuser/WPS70/responsefiles/WBI/../../IM/userinst --launcher.ini
/home/wpsuser/WPS70/responsefiles/WBI/../../IM/user-silent-install.ini -input
/home/wpsuser/WPS70/responsefiles/WBI/my_response.xml -log
/export/home/wps/wpsv7/ProcServer/logs/wps/silent_install.log
```

```
The next step is to use the manageProfiles command or the Profile
Management Tool to augment existing profiles or create a new profile to
enable the functionality provided by the feature pack. See the
Information Center articles on creating, deleting, and augmenting
profiles. Additionally, Network Deployment customers should read the
profile rules and limitations topic.
```

The 'WAS rc:0' output indicates that WebSphere Application Server was successfully installed. You could also check under `WAS_LOCATION/logs/install/log.txt` for an `INSTCONFSUCCESS` message to confirm the same.

The output 'The next step...' indicates that WebSphere Process Server was successfully installed.

What to do next

Perform post-installation tasks and verify the installation:

- Verify that the `INSTCONFSUCCESS` message appears in the *WAS_LOCATION*/logs/install/log.txt file to indicate that WebSphere Application Server was installed.

- Check the *WAS_LOCATION*/logs/wps/silent_install.log to verify that WebSphere Process Server was installed. You will see a message similar to the following if the installation was successful. You will also see the same message in the shell you used to run the run_templates script.

```
The next step is to use the manageProfiles command or the Profile
Management Tool to augment existing profiles or create a new profile to
enable the functionality provided by the feature pack. See the
Information Center articles on creating, deleting, and augmenting
profiles. Additionally, Network Deployment customers should read the
profile rules and limitations topic.
```

Starting the First steps console

After installing WebSphere Process Server, use the First steps console to start product tooling, access product documentation, or direct elements such as servers and administrative consoles related to individual profiles. A generic version of the console, plus a version for each profile in your installation are available.

Options on each console are displayed dynamically, depending on features you install and the availability of certain elements on particular operating systems. Options include verifying your installation, starting or stopping the server or deployment manager, accessing the administrative console, starting the Profile Management Tool, accessing the Samples gallery, accessing the product

documentation, or starting the migration wizard. Methods for starting the First steps console differ depending on whether it is a generic or profile-specific version.

The following sections provide detailed information on starting a First steps console based on its version and the platform used on the system:

- "Starting the generic version of the First steps console"
- "Starting a First steps console associated with a profile on Linux, UNIX, and Windows platforms"

Restrictions:

- The WebSphere Process Server Client does not have an associated First steps console. The underlying WebSphere Application Server or WebSphere Application Server Network Deployment installation has its own First steps console.

- `Windows` The First steps console might not start if you use Mozilla 2.x as your default browser and it is installed in a location containing a space in the path name. To rectify this problem, perform one of these actions:
  - Install Mozilla into a location without a space in the path name.
  - Alter the registry key to remove the space.
  - Temporarily set Internet Explorer as the default browser and then set Mozilla as the default browser. This automatically removes the space from the registry key.

Starting the generic version of the First steps console

Start the generic version of the First steps console by performing the following steps.

1. Open a command window.
2. Change to the following directory:
   - `Linux` `UNIX` `install_root/firststeps/wbi`
   - `Windows` `install_root\firststeps\wbi`

   The variable *install_root* represents the location of the WebSphere Process Server installation on Linux, UNIX, and Windows systems.
3. Issue one of the following commands to start the console:
   - `Linux` `UNIX` `./firststeps.sh`
   - `Windows` `firststeps.bat`

Fast path:

`Windows` You can also start the generic version of the console on Windows platforms by selecting **Start → Programs → IBM WebSphere → Process Server 7.0 → First steps**.

Starting a First steps console associated with a profile on Linux, UNIX, and Windows platforms

`Linux` `UNIX` `Windows` Start a First steps console associated with a profile by performing the following steps:

1. Open a command window.

2. Change to the following directory (where *profile_root* represents the installation location of the WebSphere Process Server or WebSphere Enterprise Service Bus profile):

- For WebSphere Process Server profiles:
  - `Linux` `UNIX` *profile_root*/firststeps/wbi
  - `Windows` *profile_root*\firststeps\wbi
- For WebSphere Enterprise Service Bus profiles:
  - `Linux` `UNIX` *profile_root*/firststeps/esb
  - `Windows` *profile_root*\firststeps\esb

3. Issue the **firststeps** command to start the console:

- `Linux` `UNIX` ./firststeps.sh
- `Windows` firststeps.bat

Fast path:

You can also start a version of the First steps console associated with a profile by performing one of the following tasks:

- Checking the First steps console check box on the Profile creation complete or Profile augmentation complete panel at the end of the profile creation or augmentation process.
- `Windows` When starting a First steps console associated with a WebSphere Process Server or WebSphere Enterprise Service Bus profile, by selecting **Start** → **Programs** → **IBM WebSphere** → **Process Server 7.0** → **Profiles** → *profile_name* → **First steps**.

See "Options on the First steps console" for descriptions of the options you can select from the First steps console.

Options on the First steps console

After installing WebSphere Process Server, use the First steps console to start product tooling, access product documentation, or direct elements such as servers and administrative consoles related to individual profiles. A generic version of the console, plus a version for each profile in your installation are available. Options on each console are displayed dynamically, depending on features you install and the availability of certain elements on particular operating systems. Options include verifying your installation, starting or stopping the server or deployment manager, accessing the administrative console, starting the Profile Management Tool, accessing the Samples gallery, accessing the product documentation, or starting the migration wizard.

Note: The underlying WebSphere Application Server installation has its own First steps console.

Options that are displayed on the various types of First steps consoles are summarized in Table 25 on page 61. Each option is defined in "Option descriptions" on page 61. "Usage tips" on page 63 describes which commands each option calls.

Table 25. Available options on First steps consoles

Option	Generic version	Stand-alone server profile version	Deployment manager profile version	Custom profile version
Installation verification	No	Yes	Yes	No
Start and stop the server	No	Yes	No	No
Start and stop the deployment manager	No	No	Yes	No
Administrative console	No	Yes	Yes	No
Profile Management Tool	Yes	Yes	Yes	Yes
Samples gallery	No	Yes	No	No
Information center	Yes	Yes	Yes	Yes
Migration wizard	Yes	Yes	Yes	Yes
Copyright and trademark information	Yes	No	No	No
Exit	Yes	Yes	Yes	Yes

Option descriptions

Options that are displayed on the various versions of the First steps consoles are described here:

Installation verification

Starts the installation verification test. The test consists of starting and monitoring the stand-alone server or deployment manager during its start up.

If this is the first time that you have used the First steps console since creating a stand-alone server or deployment manager profile, select **Installation verification** to verify your installation. The verification process starts the stand-alone server or deployment manager.

The **Start the server** and **Start the deployment manager** options are unavailable while the Installation Verification Tool (IVT) runs.

The IVT provides the following useful information about the stand-alone server or deployment manager:
- The name of the server process
- The name of the profile
- The profile path, which is the file path and the name of the profile
- The type of profile
- The cell name
- The node name
- The current encoding

- The port number for the administrative console
- Various informational messages that include the location of the `SystemOut.log` file and how many errors are listed within the file
- A System Health Report (only for stand-alone servers)
- A completion message

Review more information about verifying your installation in "Verifying the product installation" on page 79 and its child topics.

Start the server

Toggles to **Stop the server** when the server runs.

After selecting the **Start the server** option, an output screen is displayed with status messages. The success message informs you that the server is open for e-business. Then the menu item changes to **Stop the server** and both the **Administrative console** and **Samples gallery** options are enabled (if you installed them).

If you select the **Start the server** option, the **Installation verification** option is unavailable while the server is starting.

Start the deployment manager

Toggles to **Stop the deployment manager** when the deployment manager runs.

After selecting the **Start the deployment manager** option, an output screen is displayed with status messages. The success message informs you that the deployment manager is open for e-business. Then the menu item changes to **Stop the deployment manager** and the **Administrative console** option is enabled (if you installed it).

If you select the **Start the deployment manager** option, the **Installation verification** option is unavailable while the deployment manager runs.

Administrative console

Displayed only if you deployed the Administrative console during profile creation or augmentation. This option is unavailable until you start the stand-alone server or deployment manager.

The administrative console is a configuration editor that runs in a Web browser. The administrative console lets you work with XML configuration files for the stand-alone server or deployment manager, and all of the applications that are in the cell.

To start the administrative console, select **Administrative console**.

Avoid trouble: **Vista** **Windows 7** If you are installing the product on these operating systems, you must disable IPv6 and restart the machine to view and log on to the administrative console. See IPv6 for Microsoft® Windows®: Frequently Asked Questions for more information on disabling IPv6.

The administrative console prompts for a login name. This is not a security item, but merely a tag to identify configuration changes that you make during the session. Secure sign on is also available when administrative security is enabled.

The installation procedures in the information center caution you to write down the administrative user ID and password when security is enabled during installation. Without the ID and password, you cannot use the administrative console or scripting.

Profile Management Tool

Starts the Profile Management Tool. The tool lets you create a stand-alone server, deployment manager, or custom profile.

A *profile* consists of files that define the runtime environment for the stand-alone server or deployment manager. Each profile has its own administrative interface. A custom profile is an exception. A custom profile is an empty node that you federate into a deployment manager cell and customize. No default server processes or applications are created for a custom profile.

Each profile has its own First steps console. The location of the command to start the First steps console is within the set of files in the profile. A prompt to start the First steps console that is associated with a profile is displayed on the last panel of the Profile Management Tool.

Restriction: The Profile Management Tool cannot be used to create or augment profiles on 64-bit architectures except on the Linux on System z platform. To create profiles on other 64-bit architectures, you can use the manageprofiles command-line utility. You can also use the Profile Management Tool on these architectures if you use a 32-bit installation.

Samples gallery

Displayed only if you installed the WebSphere Process Server samples during profile creation or augmentation. This option starts the WebSphere Process Server Samples gallery in the administrative console. The option is unavailable until you start the server.

To start the Samples gallery, select **Samples gallery**.

If you did not install the WebSphere Process Server samples during the initial installation of the product, the option does not display on the First steps console. You can perform an incremental installation to add the Samples feature. After adding the Samples, the option is displayed on the First steps console.

Information center

Links you to the WebSphere Process Server online information center.

Migration wizard

Starts the WebSphere Process Server version-to-version migration wizard, which is the graphical interface to the migration tools. The version-to-version migration wizard is a graphical interface that guides you through migrating from an older version to a newer version of WebSphere Process Server. See the topic Migrating a profile using the BPM profile migration wizard for more information about this interface.

Copyright and trademark information

Shows the copyright and trademark information for WebSphere Process Server.

Exit   Closes the First steps console.

Usage tips

Table 26 on page 64 shows which commands the options on the various WebSphere Process Server First steps consoles call. For more information on selected individual commands, look up the command in the Command-line utilities section in the WebSphere Application Server Network Deployment information center:

- startServer command

- stopServer command
- startManager command
- stopManager command

The commands used to start the installation verification test, the First steps console, the Profile Management Tool, and the Migration wizard included in the WebSphere Process Server product have different names, exist in different directory locations, or perform different functions than the equivalent WebSphere Application Server Network Deployment commands. Therefore, links to those commands in the WebSphere Application Server Network Deployment information center are not provided here.

Table 26. Commands called by First steps console options

Option	Link
Installation verification	Calls the wbi_ivt command-line utility.
	The location of the installation verification test command is:
	- `Linux` `UNIX` **On Linux and UNIX platforms:** `profile_root`/bin/wbi_ivt.sh
	- `Windows` **On Windows platforms:** `profile_root`\bin\wbi_ivt.bat
Start the server	Calls the startServer command.
	The location of the startServer command is:
	- `Linux` `UNIX` **On Linux and UNIX platforms:** `profile_root`/bin/startServer.sh
	- `Windows` **On Windows platforms:** `profile_root`\bin\startServer.bat
	When you have more than one stand-alone server on the same workstation, the command starts the stand-alone server that is associated with the same profile as in the First steps console.
Stop the server	Calls the stopServer command.
	The location of the stopServer command is:
	- `Linux` `UNIX` **On Linux and UNIX platforms:** `profile_root`/bin/stopServer.sh
	- `Windows` **On Windows platforms:** `profile_root`\bin\stopServer.bat
Start the deployment manager	Calls the startManager command.
	The location of the startManager command is:
	- `Linux` `UNIX` **On Linux and UNIX platforms:** `profile_root`/bin/startManager.sh
	- `Windows` **On Windows platforms:** `profile_root`\bin\startManager.bat
	When you have more than one deployment manager on the same workstation, the command starts the deployment manager that is associated with the same profile as in the First steps console.
Stop the deployment manager	Calls the stopManager command.
	The location of the stopManager command is:
	- `Linux` `UNIX` **On Linux and UNIX platforms:** `profile_root`/bin/stopManager.sh
	- `Windows` **On Windows platforms:** `profile_root`\bin\stopManager.bat

Table 26. Commands called by First steps console options (continued)

Option	Link
Administrative console	Opens the default browser to the administrative console Web address. When you have more than one server on the same workstation, the port varies. The First steps console starts the administrative console that is associated with the same profile as in the First steps console.
Profile Management Tool	Calls the pmt command. The location of the pmt command is: • `Linux` `UNIX` **On Linux and UNIX platforms:** `install_root`/bin/ProfileManagement/pmt.sh • **On Windows platforms:** `install_root`\bin\ProfileManagement\pmt.bat
Samples gallery	Opens the default browser to the Samples Web address.
Information center	Opens the default browser to the WebSphere Process Server online information center.
Migration wizard	Calls the WebSphere Process Server version-to-version migration script to start the migration wizard. The location of the version-to-version migration script is: • `Linux` `UNIX` **On Linux and UNIX platforms:** `was_home`/bin/bpm_migration/BPMMigrate.sh • `Windows` **On Windows platforms:** `was_home`\bin\bpm_migration\BPMMigrate.bat

Installing Message Service clients

If you want to enable C, C++, or .NET applications to participate in interactions with WebSphere Process Server, you can use the Message Service clients.

About this task

The steps that you need to complete to install message service clients depends on the type of client and the type of installation you choose to use. The steps are described in the documentation for the type of client.

Procedure
• Installing Message Service Client for .NET
• Installing Message Service Client for C/C++

Installing the JNDILookup Web Service application

WebSphere Process Server maintains administered JMS objects which cannot be interpreted by non-Java clients. To allow non-Java clients to access administered objects, WebSphere Process Server provides a JNDILookup Web Service. This Web service acts as a proxy to allow non-Java clients to retrieve JMS administered objects.

Before you begin

Before installing the JNDILookup Web Service application you must ensure you have a running installation of WebSphere Process Server on your system.

About this task

If your WebSphere Process Server installation is going to be accessed by non-Java clients, you need to install the JNDILookup Web Service. This application can be installed using the administrative console as described below.

Important: After you start performing the steps below, click **Cancel** to exit if you decide not to install the application. Do not simply move to another administrative console page without first clicking **Cancel** on an application installation page.

Procedure

1. Click **Applications** → **New Application** in the console navigation tree.

   The first of two Preparing for application installation pages is displayed.

2. On the first Preparing for the application installation page, specify the path to the new application.

   a. Browse to the *install_root*/installableApps directory, and select SIBXJndiLookupEAR.ear.

   b. Click **Next**.

3. On the second Preparing for application installation page:

   a. Select whether to generate default bindings and mappings.

      Using the default bindings causes any incomplete bindings in the application to be completed with default values. Existing bindings are not altered. You can customize default values used in generating default bindings.

   b. Click **Next**.

   The Install New Application pages are displayed.

4. On Step 1: Select installation options panel, select **Deploy Web services**.

5. Click **Step 5: Summary** to go to the Summary panel.

6. On the Summary panel click **Finish**.

What to do next

Examine the application installation progress messages. If the application installs successfully, save your changes to the Master Configuration. You can now see **SIBXJndiLookup** in the list of deployed applications on the Enterprise Applications page accessed by clicking **Applications** → **Enterprise Applications** in the console navigation tree.

To start the application from the Enterprise Applications page, select **SIBXJndiLookup** and click **Start**.

Modifying a product installation

You can change the installed software packages by adding or removing features and functions using the Installation Manager.

Before you begin

Close all programs that were installed using Installation Manager before modifying. You can review additional Installation Manager documentation in the Installation Manager Information Center.

Important: During product installation or modification, you might see errors in the Installation Manager interface or log files similar to the following:

```
228 ERROR  07:41.26 Installation Manager cannot remove feature import.configLauncher.
feature from an installation package that was imported to Installation Manager.
229 ERROR  07:41.54 Installation Manager cannot remove feature import.productProviders.
feature from an installation package that was imported to Installation Manager.
```

You can safely ignore such errors.

Procedure

1. Start Installation Manager. See "Starting IBM Installation Manager manually" for more information.
2. From the Start page of the Installation Manager, click **Modify**.
3. If IBM Installation Manager is not detected on your system or if an older version is already installed, then you must continue with the installation of the latest release. Follow the on-screen instructions in the wizard to complete the installation of IBM Installation Manager.
4. In the Modify Packages wizard, select the packages that you want to modify and click **Next**.
5. Expand the list entries, select the features you want to modify in your installation, and click **Next**.
6. Review the summary information. If the summary information is incorrect, click **Back** to change your selections. If it is correct, click **Modify**.

   When the modification is complete, a page displays the status of the modification. Click **View Log File** to see the complete log.
7. Click **Finish**.
8. Close Installation Manager.

Results

Your WebSphere Process Server installation is modified.

Starting IBM Installation Manager manually

If you start the installation of your product from the launchpad program, the installation of IBM Installation Manager is performed automatically if it is not already installed on your workstation. This topic instructs how to start the tool after it is installed.

Procedure

Start Installation Manager by performing one of the following tasks:

- Linux UNIX Go to the installation directory for Installation Manager and run the command IBMIM. Refer to "Default installation directories for Installation Manager" on page 129.

- Windows From the Windows task bar, click **Start > All Programs** or **Programs > IBM Installation Manager > IBM Installation Manager**.

What to do next

Review additional Installation Manager documentation in the Installation Manager Information Center.

Installing the documentation

You can install the WebSphere Process Server Help System from the product installation launchpad on the following systems: Microsoft Windows XP, Red Hat Enterprise Linux V5, and AIX 5.3 for 64-bit PowerPC systems. After you install the WebSphere Process Server Help System, you can update your local installation with the latest documentation.

Before you begin

The topics in this section describe how to install the WebSphere Process Server Help System and product documentation on your computer. If WebSphere Process Server is installed on a system other than Microsoft Windows XP, Red Hat Enterprise Linux V5, or AIX 5.3 for 64-bit PowerPC systems, or if you prefer to view the information by way of the Internet, you can access the WebSphere Business Process Management Version 7.0 Information Center by clicking the following link: IBM WebSphere Business Process Management Version 7.0 information center.

For alternative access to the documentation set for a WebSphere Business Process Management product, including Adobe® Acrobat Portable Document Format (PDF) versions of the information, use the **Library** link on the Web page for the product. You can see a list of the product Web pages on the WebSphere Business Process Management page: BPM - Business Process Management

About this task

After you install the documentation, you can start and use the WebSphere Process Server Help System in either stand-alone mode or server mode:

*   In stand-alone mode, the WebSphere Process Server Help System acts as a personal help system.
*   In server (or information center) mode, the WebSphere Process Server Help System with the documentation acts as a public documentation server and allows other Web browsers on your network to connect to the help system on a specified port.

Having a local copy of the documentation gives you access to the information you need to install, maintain, and use the product–even when you are not connected to the Internet.

Procedure

*   To install the WebSphere Process Server Help System and documentation, see "Installing a new help system" on page 70.
*   To update the WebSphere Process Server Version 7.0 documentation if you already have the WebSphere Process Server Help System installed, see "Installing the latest documentation into a help system" on page 71.
*   To add different versions of the WebSphere Process Server documentation if you already have the WebSphere Process Server Help System installed, see "Installing different versions of documentation into a help system" on page 72.

- To add product documentation to an Eclipse-based help system other than the WebSphere Process Server Help System, see "Installing the documentation in other Eclipse-based help viewers" on page 73.

What to do next

After you have installed the IBM WebSphere Process Server Help System, you can open that help system to view product documentation. To get started with the WebSphere Process Server Help System, review the help topics in Welcome to the documentation.

To see the latest information about your product, go to WebSphere Process Server

Installing a new help system

You install the WebSphere Process Server Help System, including the product documentation, from the WebSphere Process Server launchpad.

Before you begin

You must have a working Internet connection to install the help system and documentation.

Procedure

1. Start the launchpad by navigating to the directory in which WebSphere Process Server was installed and entering one of the following commands:
   - **On Linux and UNIX platforms:** `launchpad.sh`
   - **On Windows platforms:** `launchpad.exe`
2. From the launchpad, click **Help System Installation**.
3. In the **Specify the installation location** field, type the directory in which you want the help system installed.
4. Click **Install and start the Help System**.

   The help system is installed on your computer, and you see instructions for installing the documentation.
5. Click the **Update** icon ( ) in the help system toolbar.

   You see a list of any documentation sets that are already installed.
6. Click **Next** at the bottom of the installed documentation list.

   You see a list of documentation sets to install. These sets include product documentation in different languages and can also include documentation sets for different products.
7. Click **Finish** to complete the installation.

Results

The help system is installed and started, and you can view the documentation.

What to do next

To stop the help system, see "Stopping the help system" on page 75.

Related tasks

"Uninstalling the documentation" on page 77
To uninstall the IBM WebSphere Process Server Help System (including all the documentation within it) from your local system, delete the directory in which the help system was installed.

"Stopping the help system" on page 75
Use command files on your computer to stop the help system.

Installing the latest documentation into a help system

If you have already installed the IBM WebSphere Process Server Help System, you can use the update function in the help system to install updated versions of the product documentation.

Before you begin

Installing documentation into the IBM WebSphere Process Server Help System requires a working Internet connection to download documentation.

About this task

You can use the update function to update your local installation with the latest documentation available for products in the same version of the WebSphere Business Process Management product family.

Procedure

1. Start the IBM WebSphere Process Server Help System. Follow the instructions in Starting the help system if you need assistance.

2. Click the **Update** icon ( ) in the help system toolbar.

   You see a list of any documentation sets that are already installed.

3. Click **Next** at the bottom of the installed documentation list.

   You see a list of documentation sets to install. These sets include product documentation in different languages and can also include documentation sets for different products.

4. Click **Finish** to complete the installation.

What to do next

You can view the newly installed documentation in your help system.

If the updated documentation is not displayed, stop and restart the help system to view it.

Related tasks

"Installing the documentation in other Eclipse-based help viewers" on page 73
If you are using an Eclipse-based help viewer and want to make WebSphere
Process Server documentation available for viewing there, you can configure your
viewer to view the documentation.

"Stopping the help system" on page 75
Use command files on your computer to stop the help system.

"Starting the help system" on page 75
Use command files on your computer to start the help system.

Installing different versions of documentation into a help system

You can install different versions of the product documentation in your WebSphere
Process Server Help System. For example, if you have already installed a help
system from an earlier version of the product (for example, WebSphere Process
Server Version 6.2), you can add documentation for the newer product version into
that help system.

Before you begin

Installing documentation into the IBM WebSphere Process Server Help System
requires a working Internet connection to download documentation.

Only previously installed copies of the IBM WebSphere Process Server or
WebSphere Enterprise Service Bus Help System can be used. The WebSphere
Process Server and WebSphere Enterprise Service Bus Help Systems are equivalent
(for the same version) and can be used interchangeably.

Note: Your help system must include the Update function. If you have an earlier
version of the WebSphere Process Server that does not include the Update
function, you cannot use it to update the product documentation.

About this task

To indicate which documentation you want to install, you change the
bookmarks.xml file to point to the documentation update site for the new product
version.

You can install documentation for any of the following combinations:
* Add 7.0 documentation to version 6.2 or version 6.1.2 of the WebSphere Process
  Server Help System
* Add 6.2 documentation to version 6.1.2 of the WebSphere Process Server Help
  System
* Add 6.1.2 documentation to version 6.2 of the WebSphere Process Server Help
  System
* Add non-WebSphere Business Process Management product documentation to
  the WebSphere Process Server Help System

Procedure

1. To add a different version of documentation to your help system, perform the
   following steps:
   a. Go to the plug-ins directory of your help system.

b. Within that plug-ins directory, find the Eclipse `webapp` plug-in directory, which is typically named `org.eclipse.help.webapp_<version>`. For example, the 3.1.1 version of the Eclipse webapp plug-in folder is named `org.eclipse.help.webapp_3.1.1`.

c. In that plug-in folder, open the file `bookmarks.xml` for editing.

d. Add or change the values of the site element attributes:

Table 27. Site element attributes

name (optional)	IBM Help System server
url	• For version 7.0 of the documentation: http://publib.boulder.ibm.com/ dmndhelp/downloads/v7r0mx • For version 6.2 of the documentation: http://publib.boulder.ibm.com/ dmndhelp/downloads/v6r2mx • For version 6.1.2 of the documentation: http://publib.boulder.ibm.com/ dmndhelp/downloads/

For example, to point to the version 7.0 information center, you would update the file as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<bookmarks>
 <site name="IBM Help System server"
   url="http://publib.boulder.ibm.com/dmndhelp/downloads/v7r0mx" />
</bookmarks>
```

2. Start the WebSphere Process Server Help System. Follow the instructions in Starting the help system if you need assistance.

3. Click the **Update** icon ( ) in the help system toolbar.

4. Proceed to select the documentation sets you want to install. When you are finished making your selections, confirm the documentation to be installed.

What to do next

You can view the newly installed documentation in your help system.

If the updated documentation is not displayed, stop and restart the help system to view it.

Related tasks

"Stopping the help system" on page 75
Use command files on your computer to stop the help system.

"Starting the help system" on page 75
Use command files on your computer to start the help system.

Installing the documentation in other Eclipse-based help viewers

If you are using an Eclipse-based help viewer and want to make WebSphere Process Server documentation available for viewing there, you can configure your viewer to view the documentation.

Before you begin

Installing documentation into an Eclipse-based help viewer requires a working Internet connection to download documentation. Your Eclipse-based help viewer must also be version 3.1.0 or higher.

About this task

The IBM WebSphere Process Server Help System is specially configured to download documentation from the update server for version 7.0 of WebSphere Business Process Management products. You can configure other Eclipse-based help systems to download documentation from that update server.

Procedure

1. Go to the plug-ins directory of your Eclipse-based help viewer.
2. Within that plug-ins directory, find the Eclipse webapp plug-in directory, which is typically named `org.eclipse.help.webapp_<version>`. For example, the 3.1.0 version of the Eclipse webapp plug-in folder is named `org.eclipse.help.webapp_3.1.0`.
3. In that plug-in folder, open the file `bookmarks.xml` for editing.
4. Add or change the values of the site element attributes:

Option	Description
name (optional)	update server
url	http://publib.boulder.ibm.com/dmndhelp/downloads/v7r0mx

   For example, to point to the version 7.0 information center, you would update the file as follows:
   ```
   <?xml version="1.0" encoding="UTF-8"?>
   <bookmarks>
    <site name="update server"
      url="http://publib.boulder.ibm.com/dmndhelp/downloads/v7r0mx" />
   </bookmarks>
   ```
5. Start the help system in stand-alone mode. The update function is not available in server mode. If the help system is already running, you need to stop it before restarting.
6. Click the appropriate button to update the documentation.
7. Proceed to select the documentation sets you want to install. When you are finished making your selections, confirm the documentation to be installed.

What to do next

You can view the newly installed documentation in your help system.

If the updated documentation is not displayed, stop and restart the help system to view it.

Related tasks

"Stopping the help system"
Use command files on your computer to stop the help system.

"Starting the help system"
Use command files on your computer to start the help system.

Starting the help system

Use command files on your computer to start the help system.

Before you begin

You must have a version of the help system installed on your workstation.

Procedure

- To start the help system in stand-alone mode, complete the following steps:
  1. Go to the directory into which you installed the help system.
  2. Run the appropriate help_start script:
     - **On Linux and UNIX platforms:** `help_start.sh`
     - **On Windows platforms:** `help_start.bat`

     It might take a few minutes for the system to start.
- To start the help system in server (information center) mode, complete the following steps:
  1. Go to the directory into which you installed the help system.
  2. Optional: Change the port on which the information center server starts.

     By default, the server starts on port 8888.

     If you want the server to start on a different port, edit the appropriate start script and change the -port setting:
     - **On Linux and UNIX platforms:** `IC_start.sh`
     - **On Windows platforms:** `IC_start.bat`

     For example, to use port 9876, type `-port 9876`
  3. Run the appropriate help_start script:
     - **On Linux and UNIX platforms:** `IC_start.sh`
     - **On Windows platforms:** `IC_start.bat`

Results

The help system is started.
- In stand-alone mode, a Web browser is opened to display the contents of the help system.
- In server mode, users can open a Web browser to view the help system contents.

Related tasks

"Stopping the help system"
Use command files on your computer to stop the help system.

Stopping the help system

Use command files on your computer to stop the help system.

Before you begin

You must have a version of the help system installed on your workstation.

Procedure

- To stop a help system viewer running in stand-alone mode, complete the following steps:
  1. Go to the directory into which you installed the help system.
  2. Start the appropriate script in that directory:
     - **On Linux and UNIX platforms:** `help_end.sh`
     - **On Windows platforms:** `help_end.bat`
- To stop a help system viewer running in server mode, complete the following steps:
  1. Go to the directory into which you installed the help system.
  2. Start the appropriate script in that directory:
     - **On Linux and UNIX platforms:** `IC_end.sh`
     - **On Windows platforms:** `IC_end.bat`

Results

The help system is stopped.

Related tasks

"Starting the help system" on page 75
Use command files on your computer to start the help system.

Viewing the help system

Use a Web browser to view the contents of your help system.

About this task

When the help system runs in server mode, it calls a Web application on the user-defined port and makes the help content available to any Web browser that connects to that help system. The help pages and menus are displayed in the locale of the Web browser. To change the port on which the server starts, you can change the start-up script in a text editor.

When you start the information center in stand-alone mode, the documentation is displayed automatically.

However, to view the documentation in server mode, you must complete the following steps:

Procedure

1. Open a Web browser.
2. Type the URL `http://<servername>:<port>/help` to the help pages, where *<servername>* is the host name or IP address of the system where the WebSphere Process Server Help System is installed.

   For example, if the information center is installed on the server `xyz.com` and the default port is used, you can open the information center by entering the following URL `http://xyz.ibm.com:8888/help`
3. Press Enter.

It might take a few minutes for the system to start.

Uninstalling the documentation

To uninstall the IBM WebSphere Process Server Help System (including all the documentation within it) from your local system, delete the directory in which the help system was installed.

About this task

Note that deleting the WebSphere Process Server Help System removes the help system and all documentation (including any other product documentation you have installed in this location).

Verifying the product installation

Use the installation verification tools to verify that the installation of WebSphere Process Server and the creation of the stand-alone server or deployment manager profiles were successful. A *profile* consists of files that define the runtime environment for a deployment manager or a server. Verify the core product files with the installver_wbi checksum tool. Verify each profile with the installation verification test (IVT) tool.

Before you begin

After installing WebSphere Process Server and creating a stand-alone server or deployment manager profile, you are ready to use the installation verification tools.

About this task

Use the installation verification tools to gain assurance that the product is successfully installed. WebSphere Process Server includes two installation verification tools:

- The installver_wbi checksum tool, which verifies that the WebSphere Process Server files installed on your system were installed completely. The installver_wbi command-line utility compares the checksum of each installed WebSphere Process Server file to the correct checksum value for each file and reports differences.
- The installation verification test (IVT) tool, which tests deployment manager profiles and stand-alone server profiles to make sure that the server processes can start. The IVT program scans product log files for errors and verifies core functionality of the product installation. Additionally, the IVT will perform a System Health check and generate a report for stand-alone server profiles.

To use the verification tools, perform the following steps.

Procedure

1. Run the installver_wbi command-line utility to verify that all WebSphere Process Server files are correctly installed.

   For more information, see "Verifying checksums of installed files."

2. Use the installation verification test (IVT) tool to verify the proper creation of profiles. On the First steps console, click **Installation verification** or use the wbi_ivt command-line utility.

What to do next

After installing the product and verifying the installation, you can configure the installation by creating more profiles.

Verifying checksums of installed files

After installing the product or after installing maintenance packages, you can use the installation verification utility (IVU) to compute checksums of the installed file set to verify the checksum against the checksum in the product bill of materials.

Before you begin

Installing the product also installs the IVU, which is the installver_wbi.bat command-line tool.

About this task

You use the installver_wbi.bat command-line tool to compute a checksum on the installed files and compare the checksum to the product bill of materials.

The installation verification utility tool is installed during the installation of WebSphere Process Server.

You can also use the IVU to compute a new checksum for a system after you make significant configuration changes. The installver_wbi.bat tool computes a new baseline checksum for each file in the inventory of a configured system to use to identify file changes in the later comparisons. Such a comparison is useful for detecting file tampering on the configured system, for example.

You can use the new checksums to compare installations on multiple systems. The following graphic illustrates the main use cases where you can perform product verification at any point of the product life cycle or use the inventory file, which is part of the baseline checksum feature, to provide full-file verification of a configured system.
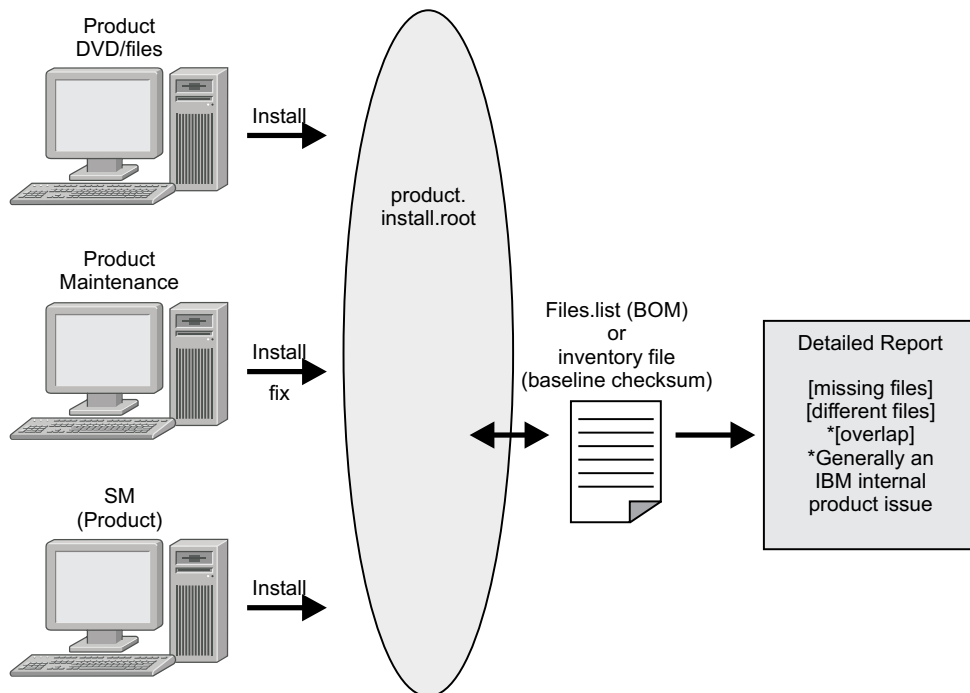
Although the most common use of the tool is to compare the product bill of materials to the installed file set, other tasks are also possible.

To verify the checksums of installed files, perform the following steps.

Procedure

- Verify the installed files against the bill of materials.

  See "Verifying against the bill of materials" on page 82 for more information.
- Create and use a new baseline checksum.

  See "Computing a new baseline checksum for an inventory of configured files" on page 85 for more information.
- Exclude files and components from the comparison.

  See "Excluding files from a checksum comparison" on page 88 for more information.
- Include only specific files and components in the comparison.

  See "Comparing specific file and component checksums" on page 91 for more information.
- Change the default message digest algorithm for computing checksums.

  See "Changing the default message digest algorithm for the installver_wbi command-line utility" on page 94 for more information.
- Handle out-of-memory conditions.

  See "Handling out-of-memory situations" on page 95 for more information.
- Verify the installver_wbi.bat command files.

Results

When you are satisfied that your installed or updated file set matches the product bill of materials, you are finished verifying the product files.

If you detect a problem, see if the problem is a known problem by checking the WebSphere Process Server Support Web site.

The IVU performs the tasks using the logic described in the following graphic:
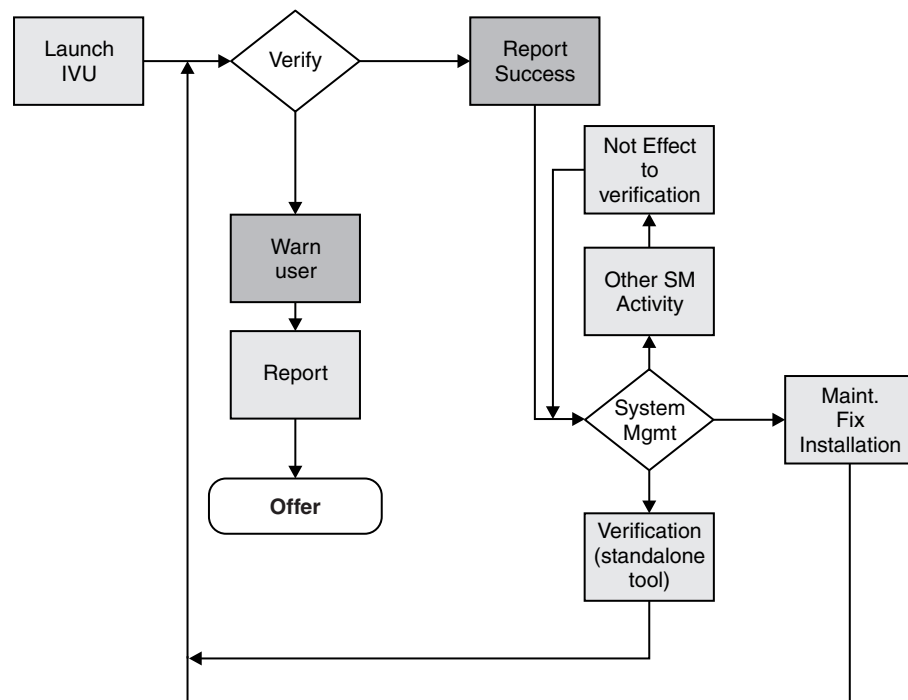
Verifying against the bill of materials

After installation of the product, verify actual checksums of installed files against a bill of materials that ships with the product. If the checksums match, the installed product is installed correctly. If the checksums differ, review the differences to determine whether a problem exists.

Before you begin

Complete the product installation before attempting to compare checksums of the installed files to the shipped bill of materials.

About this task

Use the installver_wbi command-line utility to compare a set of bill-of-material files against a checksum of the installed files to verify that all installed files are correct. The product includes a bill-of-materials file for each component to provide this system of verifying installation files.

The installver_wbi command-line utility dynamically generates a list of total components found in the installation.

The installver_wbi command file is located in the `bin` directory of the installation root directory:

- `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/bin/ installver_wbi.sh
- `Windows` **On Windows platforms:** *install_root*\bin\installver_wbi.bat

Change directories to the `bin` directory to start the installver_wbi utility from the command line.

To check the bill of materials against the installed file system, perform the following steps.

Procedure

- To compare the checksum of product files to the correct checksum in the bill-of-material files, type the following command:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/bin/ installver_wbi.sh
  - `Windows` **On Windows platforms:** *install_root*\bin\installver_wbi.bat
- To compare checksums and display trace results, type the following command:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** ./installver_wbi.sh -trace
  - `Windows` **On Windows platforms:** installver_wbi.bat -trace
- To display information about how to use the installver_wbi command-line utility, type the following command:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** ./installver_wbi.sh -help
  - `Windows` **On Windows platforms:** installver_wbi.bat -help

- To compare checksums and include only specified files and components in the comparison, see "Comparing specific file and component checksums" on page 91. You can compare only the files and components that you list in the command.
- To compare checksums and ignore the list of files to exclude, type the following command:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** `./installver_wbi.sh -ignoreuserexclude`
  - `Windows` **On Windows platforms:** `installver_wbi.bat -ignoreuserexclude`

  For information about specifying a list of files to exclude from the bill of materials checksum, see "Excluding files from a checksum comparison" on page 88.
- To compare checksums and ignore all IBM-excluded files, type the following command:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** `./installver_wbi.sh -ignoreibmexclude`
  - `Windows` **On Windows platforms:** `installver_wbi.bat -ignoreibmexclude`

Results

When you issue one of the checksum commands from the *install_root*/bin directory, the status of the command is displayed on the terminal console.

Logging results: The installver_wbi command-line utility creates messages for each component. It also reports overall success based on the verification of all components in the bill of materials. The following messages indicate completion:
- I CWNVU0400I: [ivu] Total issues found : 625
- I CWNVU0340I: [ivu] Done.

The messages report the total number of issues found. If the issue count is zero, all of the components exist and no problems exist. The installver_wbi utility logs the results of the command to the *install_root*/logs/installver.log file if you use the **-log** parameter without specifying a file name for the log.

You can redirect the output using the -log parameter and an argument. The directory that you specify must already exist. For example: `./installver_wbi.sh -log /tmp/waslogs/my_installver.log`

Example

The following command produces this example, which shows the results of comparing the installed product against the product bill of materials.
- `Linux` `UNIX` **On Linux and UNIX platforms:** `./installver_wbi.sh`
- `Windows` **On Windows platforms:** `installver_wbi.bat`

Example output from components with errors

This example shows errors that the comparison finds.

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is E:\WPS61\
I CWNVU0300I: [ivu] The total number of user excluded files found is 38.
I CWNVU0300I: [ivu] The total number of IBM excluded files found is 82.
```

```
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 441
I CWNVU0270I: [ivu] Gathering installation root data.
W CWNVU0280W: [ivu] Component mismatch: expected mismatchcomponentname
  but found mismatchingname
I CWNVU0360I: [ivu] The following bill of materials issue is found for component
  nullvaluesample: Hash must not be null or an empty string.
I CWNVU0360I: [ivu] The following bill of materials issue is found for component
  nullvaluesample: Name must not be null or an empty string.
I CWNVU0360I: [ivu] The following bill of materials issue is found for component
  nullvaluesample: Hash must not be null or an empty string.
I CWNVU0360I: [ivu] The following bill of materials issue is found for component
  nullvaluesample: Permission must not be null or an empty string.
I CWNVU0360I: [ivu] The following bill of materials issue is found for component
  symlinksample: Hash must not be null or an empty string.
I CWNVU0290I: [ivu] Starting the verification for 6 components.

I CWNVU0470I: [ivu] Starting to analyze: _binarycomponentsample
I CWNVU0480I: [ivu] Done analyzing: _binarycomponentsample

I CWNVU0470I: [ivu] Starting to analyze: nullvaluesample
I CWNVU0430I: [ivu] The following file is missing: testpath
I CWNVU0390I: [ivu] Component issues found : 1
I CWNVU0480I: [ivu] Done analyzing: nullvaluesample

I CWNVU0470I: [ivu] Starting to analyze: overlapbinarycomponentsample
W CWNVU0422W: [ivu] The following file is overlapped: lib/binaryTest.jar
W CWNVU0425W: [ivu] The overlap is caused by: _binarycomponentsample
I CWNVU0390I: [ivu] Component issues found : 1
I CWNVU0480I: [ivu] Done analyzing: overlapbinarycomponentsample

I CWNVU0470I: [ivu] Starting to analyze: regularcomponentsample
I CWNVU0440I: [ivu] The following file is different: lib/different.jar
I CWNVU0410I: [ivu] fc19318dd13128ce14344d066510a982269c241b is the
checksum in the bill of materials.
I CWNVU0420I: [ivu] 517d5a7240861ec297fa07542a7bf7470bb604fe is the
checksum on the file system.
I CWNVU0440I: [ivu] The following file is different: lib/ibmtemplateexclude.jar
I CWNVU0410I: [ivu] d3ac7a4ef1a8ffb4134f2f6e7f3c0d249d74b674 is the
checksum in the bill of materials.
I CWNVU0420I: [ivu] d3ac7a4ef1a838b4134f2f6e7f3c0d249d74b674 is the
checksum on the file system.
I CWNVU0430I: [ivu] The following file is missing: lib/missing.jar
I CWNVU0440I: [ivu] The following file is different: lib/usertemplateexclude.jar
I CWNVU0410I: [ivu] 12dea96fec20593566ab75ff2c9949596833adc9 is the
checksum in the bill of materials.
I CWNVU0420I: [ivu] 12dea96fec20593566ab75692c9949596833adc9 is the
checksum on the file system.
I CWNVU0430I: [ivu] The following file is missing: missingfilebutwithbaddirectory/
missingBadDirectory.jar
I CWNVU0390I: [ivu] Component issues found : 5
I CWNVU0480I: [ivu] Done analyzing: regularcomponentsample

I CWNVU0470I: [ivu] Starting to analyze: symlinksample
I CWNVU0480I: [ivu] Done analyzing: symlinksample

I CWNVU0400I: [ivu] Total issues found : 7
I CWNVU0340I: [ivu] Done.
```

Example output from a typical successful installation

This example shows typical results from checking a successful installation.

Carefully examine an issue before assuming that the issue is a problem.

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is E:\WPS61\
I CWNVU0300I: [ivu] The total number of user excluded files found is 38.
I CWNVU0300I: [ivu] The total number of IBM excluded files found is 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 441
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0290I: [ivu] Starting the verification for 439 components.

I CWNVU0470I: [ivu] Starting to analyze: ArtifactLoaderImpl
I CWNVU0480I: [ivu] Done analyzing: ArtifactLoaderImpl

I CWNVU0470I: [ivu] Starting to analyze: activity.impl
I CWNVU0480I: [ivu] Done analyzing: activity.impl

I CWNVU0470I: [ivu] Starting to analyze: activity.session.impl
I CWNVU0480I: [ivu] Done analyzing: activity.session.impl

I CWNVU0470I: [ivu] Starting to analyze: acwa
I CWNVU0480I: [ivu] Done analyzing: acwa

I CWNVU0470I: [ivu] Starting to analyze: adapter
I CWNVU0480I: [ivu] Done analyzing: adapter
...


I CWNVU0470I: [ivu] Starting to analyze: workspace
I CWNVU0480I: [ivu] Done analyzing: workspace

I CWNVU0470I: [ivu] Starting to analyze: workspace.query
I CWNVU0480I: [ivu] Done analyzing: workspace.query

I CWNVU0470I: [ivu] Starting to analyze: wps.rt.bundle
I CWNVU0480I: [ivu] Done analyzing: wps.rt.bundle

I CWNVU0470I: [ivu] Starting to analyze: wps.wccm.bundle
I CWNVU0480I: [ivu] Done analyzing: wps.wccm.bundle

I CWNVU0470I: [ivu] Starting to analyze: wpsnd
I CWNVU0480I: [ivu] Done analyzing: wpsnd

I CWNVU0470I: [ivu] Starting to analyze: wsadie.bundle
I CWNVU0480I: [ivu] Done analyzing: wsadie.bundle

I CWNVU0470I: [ivu] Starting to analyze: wsba.impl
I CWNVU0480I: [ivu] Done analyzing: wsba.impl

I CWNVU0400I: [ivu] Total issues found : 0
I CWNVU0340I: [ivu] Done.
```

Computing a new baseline checksum for an inventory of configured files

After installation, you can verify the actual checksums of installed files against a bill of materials that ships with the product. After configuring your system, create a checksum so that you can compare the system periodically to the checksum. Use the result to analyze changes to your configured system.

Before you begin

After configuring the product, save a new baseline checksum to establish a new checksum standard for your system.

About this task

You can use the installver_wbi command-line utility to create and compare an inventory of configured files to the currently installed files.

The installver_wbi command-line utility can compute a new baseline checksum for the inventory of all files in the installation root directory. Running the command-line utility stores the new checksum by default in the `sys.inv` file within the current working directory. You can specify a different file path and file name. Create the file outside of the installation root directory or exclude the file from comparisons.

Later, compare the checksums in the `sys.inv` file (or the file that you specified when creating the inventory) to the checksums of the currently installed files to see what files have changed.

The baseline checksum report identifies missing files, additional files, and changed files.

The installver_wbi command-line utility is located in the `bin` directory of the installation root directory:

- `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/bin/ installver_wbi.sh
- `Windows` **On Windows platforms:** *install_root*\bin\installver_wbi.bat

Change directories to the `bin` directory to start the installver_wbi utility from the command line.

To compute a new baseline checksum for an inventory of configured files, perform the following steps.

Procedure

- Create an inventory list of the files that are currently installed in the installation root directory:

  - `Linux` `UNIX` **On Linux and UNIX platforms:** ./installver_wbi.sh -createinventory

  - `Windows` **On Windows platforms:** installver_wbi.bat -createinventory

  `Windows` For example, the following messages might display on a Windows system when you issue the `installver_wbi.bat -createinventory` command to create the default *install_root*\bin\sys.inv file:

```
W CWNVU0320W: [ivu] The
C:\IBM\WebSphere\ProcServer\bin\sys.inv
inventory file is within the product installation root directory:
C:\IBM\WebSphere\ProcServer.

Create the file outside of the installation root directory to omit the file from the
 verification.
I CWNVU0300I: [ivu] The total number of user excluded files found are 2.
I CWNVU0300I: [ivu] The total number of IBM excluded files found are 78.
I CWNVU0310I: [ivu] Creating the following inventory file:
C:\IBM\WebSphere\ProcServer\bin\sys.inv
I CWNVU0460I: [ivu] The utility is running.
```

  When it finishes running, a completion message is displayed:

```
I CWNVU0340I: [ivu] Done.
```

The sys.inv contains the new inventory, as shown in this Windows system example:

```
#C:\IBM\WebSphere\AppServer\
#2005.10.10_06.24.06PM_EDT
#user_ID
#-createinventory -log
241fe4e309abfd8f2c5911216dbabd61dd4751a6
   |_jvm\bin\appletviewer.exe
   |42032
   |2004.10.28 05.37.02AM EDT
e00c6ea688ab67e004ec6cfac26ec48541a5b9ff
   |_jvm\bin\dbghelp.dll
   |712192
   |2004.10.28 05.36.50AM EDT
916e244deeb44b9d3218aafa3b56c8680aa31f2f
   |_jvm\bin\extcheck.exe
   |42040
   |2004.10.28 05.37.02AM EDT
...
7fc3bb38e8b90fed05cd0440953000c2cc965b44
   |web\spidocs\stylesheet.css
   |1240
   |2005.10.09 12.14.17AM EDT
22706a0d900c52f1c015c870ddeee25581c5d57b
   |web\spidocs\toHTML\index.html
   |867
   |2005.10.09 12.14.17AM EDT
```

- Create the inventory file in a directory outside of the installation root directory to exclude the inventory file from the comparison.

  - **`Linux`** **`UNIX`** **On Linux and UNIX platforms:** `./installver_wbi.sh -createinventory /tmp/system.inv`

  - **`Windows`** **On Windows platforms:** `installver_wbi.bat -createinventory "C:\temp\system.inv"`

- Compare the inventory list to files that are currently installed in the installation root directory:

  - **`Linux`** **`UNIX`** **On Linux and UNIX platforms:** `./installver_wbi.sh -compare`

  - **`Windows`** **On Windows platforms:** `installver_wbi.bat -compare`

  If you created the inventory file somewhere other than the default location, use the following syntax:

  - **`Linux`** **`UNIX`** **On Linux and UNIX platforms:** `./installver_wbi.sh -compare /tmp/system.inv`

  - **`Windows`** **On Windows platforms:** `installver_wbi.bat -compare "C:\temp\system.inv"`

- Compare and display trace results:

  - **`Linux`** **`UNIX`** **On Linux and UNIX platforms:** `./installver_wbi.sh -compare -trace`

  - **`Windows`** **On Windows platforms:** `installver_wbi.bat -compare -trace`

- Compare and exclude specified files from the inventory comparison:

  - **`Linux`** **`UNIX`** **On Linux and UNIX platforms:** `./installver_wbi.sh -compare -exclude` *fn1;fn2;fn3;...*

  - **`Windows`** **On Windows platforms:** `installver_wbi.bat -compare -exclude` *fn1;fn2;fn3;...*

- Compare and include only specified files in the inventory comparison:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** `./installver_wbi.sh -compare -include` *fn1*`;`*fn2*`;`*fn3*`;...`
  - `Windows` **On Windows platforms:** `installver_wbi.bat -compare -include` *fn1*`;`*fn2*`;`*fn3*`;...`

Results

When you issue an installver_wbi command from the *install_root*/bin directory, the status of the command is displayed on the terminal console. To create a log, use the -log parameter.

Excluding files from a checksum comparison

Specify individual files to exclude from a comparison, specify individual components to exclude, or create a single configurable properties file to specify a list of files to exclude from the bill of materials verification.

Before you begin

Install the product before comparing checksums and using exclusion properties.

About this task

You can use exclusion properties of the installver_wbi command-line utility to exclude files from a checksum comparison.

By default, IBM excludes some files from the checksum comparison. You can also exclude files. The number of files excluded is reported within the first few messages. For example:

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is ...
I CWNVU0300I: [ivu] The total number of user excluded files found are 0.
I CWNVU0300I: [ivu] The total number of IBM excluded files found are 82.
...
```

Several methods are provided to exclude files from the comparison.

The installver_wbi command file is located in the `bin` directory of the installation root directory:
- `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/bin/installver_wbi.sh
- `Windows` **On Windows platforms:** *install_root*\bin\installver_wbi.bat

Change directories to the `bin` directory to start the installver_wbi utility from the command line.

To exclude files from a checksum comparison, perform the following steps.

Procedure

- To exclude all the files within one or more components from the comparison, type the following command:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** `./installver_wbi.sh -excludecomponent` *comp1*`;`*comp2*`;`*comp3*`;...`

– `Windows` **On Windows platforms:** `installver_wbi.bat -excludecomponent` *`comp1;comp2;comp3;...`*

`Linux` `UNIX` For example, you might exclude the prereq.wccm component to avoid known but acceptable issues in the component:

`./installver_wbi.sh -log -excludecomponent prereq.wccm`

The resulting messages show the exclusion:

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is E:\WPS61\
I CWNVU0300I: [ivu] The total number of user excluded files found is 38.
I CWNVU0300I: [ivu] The total number of IBM excluded files found is 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 441
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0290I: [ivu] Starting the verification for 439 components.
...
I CWNVU0400I: [ivu] Total issues found : 0
I CWNVU0340I: [ivu] Done.
```

- To exclude certain files from the comparison, type the following command:

  – `Linux` `UNIX` **On Linux and UNIX platforms:** *`install_root`*`/bin/installver_wbi.sh -exclude` *`fn1;fn2;fn3`*

  – `Windows` **On Windows platforms:** *`install_root`*`\bin\installver_wbi.bat -exclude` *`fn1;fn2;fn3`*

  For example, suppose that you want to include only the prereq.wccm component for comparison, but you want to exclude specific files that were missing when you previously ran that comparison:

```
...
I CWNVU0470I: [ivu] Starting to analyze: prereq.wccm
I CWNVU0430I: [ivu] The following file is missing:
web/configDocs/activitysessionejbext/ActivitySessionEJBJarExtension.html
I CWNVU0430I: [ivu] The following file is missing:
web/configDocs/activitysessionejbext/ActivitySessionEnterpriseBeanExtension.html
I CWNVU0430I: [ivu] The following file is missing:
web/configDocs/activitysessionejbext/ContainerActivitySession.html
...
```

`Windows` Here is an example of excluding those missing files that are highlighted files in the previous example:

```
installver_wbi.bat -log -includecomponent prereq.wccm -exclude web\configDocs\activitysessionejbext\
ActivitySessionEJBJarExtension.html;web\configDocs\activitysessionejbext\
ActivitySessionEnterpriseBeanExtension.html
```

Tip: `Windows` **On Windows platforms:** Use Windows-style slashes or UNIX-style slashes to delimit directories.

The result shows that the excluded files were not compared:

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is ...
I CWNVU0300I: [ivu] The total number of user excluded files found are 0.
I CWNVU0300I: [ivu] The total number of IBM excluded files found are 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0260I: [ivu] The total number of components found is: 285
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0290I: [ivu] Starting the verification for 1 components.

I CWNVU0470I: [ivu] Starting to analyze: prereq.wccm
I CWNVU0430I: [ivu] The following file is missing:
web/configDocs/activitysessionejbext/ContainerActivitySession.html
```

```
...
I CWNVU0390I: [ivu] Component issues found : 623
I CWNVU0480I: [ivu] Done analyzing: prereq.wccm

I CWNVU0400I: [ivu] Total issues found : 623
I CWNVU0340I: [ivu] Done.
```

If the two files were in the comparison, they would be in the list and the count would be 625, as in the previous example.

Tip: The highlighted line in the example is reserved for excluded files listed in the user template file, as described in the next step. The highlighted line does not count files that you list in the installver_wbi command line with the -exclude parameter.

- To compare checksums and exclude certain files from the comparison by creating and using a user template file, perform the following steps. A configurable properties file is available to specify a list of files to exclude from the bill of materials verification.

  1. Create an empty template file by typing the following command.

     – Linux UNIX **On Linux and UNIX platforms:** *install_root*/bin/installver_wbi.sh *template_name* -createtemplate

     – Windows **On Windows platforms:** *install_root*\bin\installver_wbi.bat *template_name* -createtemplate

     Windows For example, create the default user template file on a Windows system:

     ```
     installver_wbi.bat -createtemplate
     I CWNVU0200I: [ivu] Creating template:
     C:\IBM\WebSphere\ProcServer\profiles\
     Dmgr01\properties\ivu_user.template
     I CWNVU0340I: [ivu] Done.
     ```

     The ivu_user.template file is created in the properties directory of the default profile, which, in this case, is a deployment manager profile.

     The -template_name parameter is optional. However, a template file must reside in the properties directory of the default profile, such as the *install_root*/profiles/Dmgr01/properties directory.

  2. List files to exclude in the template file.

     The properties file has the following format:

     ```
     <template>
      <componentfiles componentname="name_of_component">
        <file>
          <relativepath action="exclude">file_name</relativepath>
        </file>
      </componentfiles>
     </template>
     ```

     For example, list the component and files from the previous example:

     ```
     <template>
      <componentfiles componentname="prereq.wccm">
       <file>
        <relativepath action="exclude">
     web/configDocs/activitysessionejbext/    \
     ActivitySessionEnterpriseBeanExtension.html
        </relativepath>
       </file>
       <file>
        <relativepath action="exclude">
     web/configDocs/activitysessionejbext/    \
     ActivitySessionEJBJarExtension.html
     ```

```
          </relativepath>
         </file>
        </componentfiles>
       </template>
```

> **Tip:** Do not use quotation marks or double quotation marks to delimit a file name.

3. Use the template file to exclude files from the comparison:

    For example:

    ```
    installver_wbi.bat -log
    ```

    If the ivu_user.template file exists in the properties directory of the default profile, the installver_wbi command-line utility uses it.

    The result shows that some user files are excluded:

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is ...
I CWNVU0300I: [ivu] The total number of user excluded files found are 2.
I CWNVU0300I: [ivu] The total number of IBM excluded files found are 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 285
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0290I: [ivu] Starting the verification for 1 components.

I CWNVU0470I: [ivu] Starting to analyze: prereq.wccm
I CWNVU0430I: [ivu] The following file is missing:
web/configDocs/activitysessionejbext/ContainerActivitySession.html

...
I CWNVU0430I: [ivu] The following file is missing:
web/configDocs/wssecurity/generator-binding.html
I CWNVU0390I: [ivu] Component issues found : 623
I CWNVU0480I: [ivu] Done analyzing: prereq.wccm

I CWNVU0400I: [ivu] Total issues found : 623
I CWNVU0340I: [ivu] Done.
```

Results

When you run one of the checksum commands from the *install_root*/bin directory, the status of the command is displayed on the terminal console or in a log file.

Comparing specific file and component checksums

Specify individual files or components to include in the bill of materials verification.

Before you begin

Complete the product installation before attempting to compare checksums of individual files and components.

About this task

You can use inclusion properties to specify individual files and components.

By default, IBM includes all files in the checksum comparison except for the IBM excluded files. The displayed output will be similar to the following:

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is E:\WPS61\
I CWNVU0300I: [ivu] The total number of user excluded files found are 0.
I CWNVU0300I: [ivu] The total number of IBM excluded files found are 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 441
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0290I: [ivu] Starting the verification for 441 components.

I CWNVU0470I: [ivu] Starting to analyze: activity
I CWNVU0480I: [ivu] Done analyzing: activity
```

...

Several methods are provided to include only certain files in the comparison.

The installver_wbi command file is located in the `bin` directory of the installation root directory:

- [Linux] [UNIX] **On Linux and UNIX platforms:** *install_root*/bin/ installver_wbi.sh

- [Windows] **On Windows platforms:** *install_root*\bin\installver_wbi.bat

Change directories to the `bin` directory to start the installver_wbi utility from the command line.

To compare specific file and component checksums, perform the following steps.

Procedure

- To include only specified components in a checksum comparison, type the following command.

  - [Linux] [UNIX] **On Linux and UNIX platforms:** ./installver_wbi.sh -includecomponent *comp1*;*comp2*;*comp3*;...

  - [Windows] **On Windows platforms:** installver_wbi.bat -includecomponent *comp1*;*comp2*;*comp3*;...

  For example, you might include the activity component:

  - [Linux] [UNIX] **On Linux and UNIX platforms:** ./installver_wbi.sh -log -includecomponent activity

  - [Windows] **On Windows platforms:** installver_wbi.bat -log -includecomponent activity

  The resulting messages show the inclusion. The displayed output will be similar to the following:

```
I CWNVU0160I: [ivu] Verifying.
I CWNVU0170I: [ivu] The installation root directory is ...
I CWNVU0300I: [ivu] The total number of user excluded files found are 0.
I CWNVU0300I: [ivu] The total number of IBM excluded files found are 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 285
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0290I: [ivu] Starting the verification for 1 components.

I CWNVU0470I: [ivu] Starting to analyze: activity
```

```
I CWNVU0480I: [ivu] Done analyzing: activity

I CWNVU0400I: [ivu] Total issues found : 0
I CWNVU0340I: [ivu] Done.
```

- To include only specified files in the checksum comparison, type the following command.

  - **On Linux and UNIX platforms:** *install_root*/bin/ `installver_wbi.sh -include` *fn1*;*fn2*;*fn3*

  - **On Windows platforms:** *install_root*\bin\installver_wbi.bat `-include` *fn1*;*fn2*;*fn3*

  For example, you might include only the `properties/version/proxy.server.component` file, which was changed to generate the checksum difference in this example.

  -

    ```
    installver_wbi.bat -log -include properties\version\proxy.server.component
    ```

  The result shows that the included file was in the comparison, which scanned 285 components looking for all components that refer to the file. The displayed output will be similar to the following:

```
I CWNVU0160I: [ivu] Verifying.
...
I CWNVU0300I: [ivu] The total number of user excluded files found are 0.
I CWNVU0300I: [ivu] The total number of IBM excluded files found is 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 285
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0290I: [ivu] Starting the verification for 285 components.

I CWNVU0470I: [ivu] Starting to analyze: activity
I CWNVU0480I: [ivu] Done analyzing: activity
...
I CWNVU0470I: [ivu] Starting to analyze: proxy.server
I CWNVU0440I: [ivu] The following file is different: properties/version/proxy.server.component
I CWNVU0410I: [ivu] f385fc95977092e0482d52f9d1d5bebbc39fbb10 is the checksum in the bill of materials.
I CWNVU0420I: [ivu] b43bda7f1e7202d1f9495fc74ac14b8d85830aab is the checksum on the file system.
I CWNVU0390I: [ivu] Component issues found : 1
I CWNVU0480I: [ivu] Done analyzing: proxy.server
...
I CWNVU0400I: [ivu] Total issues found : 1
I CWNVU0340I: [ivu] Done.
```

If you know that a file is in only one component, you can speed up the comparison by restricting the comparison of the file to the relevant component. For example:

  -

```
installver_wbi.bat -log -includecomponent proxy.server -include properties\version\proxy.server.component
```

The result shows that the comparison was restricted to one component. The displayed output will be similar to the following:

```
I CWNVU0160I: [ivu] Verifying.
...
I CWNVU0300I: [ivu] The total number of user excluded files found are 0.
I CWNVU0300I: [ivu] The total number of IBM excluded files found is 82.
I CWNVU0185I: [ivu] Searching component directory for file listing: files.list
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0260I: [ivu] The total number of components found is: 285
I CWNVU0270I: [ivu] Gathering installation root data.
I CWNVU0460I: [ivu] The utility is running.
I CWNVU0290I: [ivu] Starting the verification for 1 components.
```

```
I CWNVU0470I: [ivu] Starting to analyze: proxy.server
I CWNVU0440I: [ivu] The following file is different: properties/version/proxy.server.component
I CWNVU0410I: [ivu] f385fc95977092e0482d52f9d1d5bebbc39fbb10 is the checksum in the bill
 of materials.
I CWNVU0420I: [ivu] b43bda7f1e7202d1f9495fc74ac14b8d85830aab is the checksum on the file
 system.
I CWNVU0390I: [ivu] Component issues found : 1
I CWNVU0480I: [ivu] Done analyzing: proxy.server

I CWNVU0400I: [ivu] Total issues found : 1
I CWNVU0340I: [ivu] Done.
```

Results

When you issue one of the checksum commands from the *install_root*/bin
directory, the status of the command is displayed on the terminal console or in a
log file.

Changing the default message digest algorithm for the installver_wbi command-line utility

You can change the default message digest algorithm for a checksum comparison
of installed files. You must edit the installver_wbi command script to change the
algorithm.

Before you begin

Install the product before attempting to change the default message digest
algorithm from SHA to MD5.

Also, verify the product files with the installver_wbi command-line utility before
you change the command file.

About this task

The default message digest algorithm is one of the secure hash algorithms (SHA)
that are part of the Secure Hash Standard (SHS) from the National Institute of
Standards and Technology (NIST). SHA-1 is the standard hash function of the U.S.
government. For more information, see the Federal Information Processing
Standards (FIPS) Web page at http://csrc.nist.gov/publications/fips/index.html,
and view the publication FIPS 180-2.

For more information about WebSphere Process Server compliance with FIPS, see
Federal Information Processing Standards.

Also available is the older MD5 message digest algorithm. MD5 is a deprecated
type of message algorithm that is not as secure as SHA and is provided only for
compatibility with earlier versions.

Change the default message digest algorithm from SHA to MD5 only if necessary.
Edit the installver_wbi.bat file or the installver_wbi.sh file to make the change.
Changing the algorithm invalidates the SHA-based checksums in the product bill
of materials. For this reason, verify the product files before changing the message
digest algorithm.

To change the default message digest algorithm, perform the following steps.

Procedure

1. Edit the installver_wbi command script:

    - `Linux` `UNIX` **On Linux and UNIX platforms:** Edit the
    install_root/bin/installver_wbi.sh file.

    - `Windows` **On Windows platforms:** Edit the *install_root*\bin\
    installver_wbi.bat file.

2. Add the following environmental property to the script file:

    ```
    -Dchecksum.type=MD5
    ```

    The default value is:

    ```
    -Dchecksum.type=SHA
    ```

3. Save your changes.

Results

After you change the algorithm, run the installver_wbi command-line utility to
verify that it works correctly.

Handling out-of-memory situations

Memory requirements for using the installver_wbi command-line utility are related
to the size of the installed file set for the product. For the basic verification
scenario, comparing an installed file set with the provided bill of materials might
require a maximum heap size of 128 MB to 256 MB.

About this task

If you need more memory for either a product verification or a baseline checksum
verification, you must increase the maximum heap size setting for your Java
Virtual Machine (JVM) by including a setting in the installver command script.
(The installver_wbi command calls the installver command script.)

To handle out-of-memory situations, perform the following steps.

Procedure

1. Edit the installver command script:

    - `Linux` `UNIX` **On Linux and UNIX platforms:** Edit the
    install_root/bin/installver.sh file.

    - `Windows` **On Windows platforms:** Edit the *install_root*\bin\
    installver.bat file.

2. Add or increase the maximum heap size setting:

    - `Linux` `UNIX` **On Linux and UNIX platforms:** Change the following
    line:

    ```
    "$JAVA_HOME"/bin/java \
    ```

    to:

    ```
    "$JAVA_HOME"/bin/java -Xmx256M \
    ```

    - `Windows` **On Windows platforms:** Change the following line:

    ```
    "%JAVA_HOME%\bin\java" "-Dproduct.home=%WAS_HOME%"
    ```

    to:

```
"%JAVA_HOME%\bin\java" -Xmx256M "-Dproduct.home=%WAS_HOME%"
```

3. Save your changes.

Results

After you change the setting, run the installver_wbi command-line utility to verify that it works correctly.

Coexisting with other WebSphere product installations

An installation of WebSphere Process Server, version 7.0 can coexist on the same system with installations of any version of WebSphere Enterprise Service Bus, WebSphere Process Server, and with certain versions of selected WebSphere products.

An installation of WebSphere Process Server, version 7.0 can run on the same system at the same time as installations of one or more of the following supported products and versions:

- IBM WebSphere Process Server, versions 7.0, 6.2, 6.1.x, and 6.0.x
- IBM WebSphere Enterprise Service Bus, versions 7.0, 6.2, 6.1.x, and 6.0.x
- IBM WebSphere Application Server, versions 7.0, 6.1, 6.0.x, and 5.x
- IBM WebSphere Application Server Network Deployment, versions 7.0, 6.1, 6.0.x, and 5.x
- IBM WebSphere Business Integration Server Foundation, version 5.x
- `Linux` `UNIX` `Windows` IBM WebSphere Application Server Enterprise, version 5.0.x

When configuring coexistence, you must address any port conflicts that occur to avoid communication errors. For information about port number settings, see Port number settings in WebSphere Application Server versions.

Each version of the server must have a distinct database.

Do not confuse coexistence with *migration*, *updating*, or *interoperation*:

- *Migration* is copying the configuration from a previous release of WebSphere Process Server into a new release. If you are installing WebSphere Process Server, version 7.0 on a system that already has a prior version of WebSphere Process Server or WebSphere ESB installed and you intend to migrate to the newer version of WebSphere Process Server or WebSphere ESB, see Migrating to WebSphere Process Server for more information.
- *Updating* is replacing out-of-date files or data of an existing installation with current information. Refresh packs, interim fixes, and fix packs are examples of updates.
- *Interoperation* is exchanging data between two different systems, such as coexisting product installations. This version of WebSphere Process Server is generally interoperable with many previous versions. To support interoperability, you need apply the latest fix levels. See Planning for interoperability between WebSphere Process Server and other WebSphere Application Server products for more information.

Installing WebSphere Process Server or the WebSphere Process Server Client to coexist with existing installations of various WebSphere products

Use this procedure to install WebSphere Process Server on a system with an existing installation of WebSphere Process Server, the WebSphere Process Server Client, WebSphere Enterprise Service Bus, or a supported version of WebSphere Application Server or WebSphere Application Server Network Deployment. This procedure assumes that you are starting the installation process from the launchpad application.

Before you begin

Before you can install WebSphere Process Server, perform the following tasks:

- Review the list of prerequisites for installing the product in the topic "Prerequisites for installing WebSphere Process Server" on page 29. Of particular importance are operating system and software prerequisite levels. Although the installation process automatically checks for prerequisite operating system patches, review the prerequisites at http://www.ibm.com/support/docview.wss?uid=swg27006205 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. It also lists the required levels of all prerequisite software.

- Because the launchpad is a Web application, ensure that you have a supported version of a Web browser installed.

  `Linux` `UNIX` `Windows` The platform-specific topics under Preparing the operating system for installation in the WebSphere Application Server Network Deployment information center contain detailed instructions for installing supported Web browsers on all platforms.

About this task

When you start the installation process using the launchpad application and are installing the product together with a new installation of WebSphere Application Server Network Deployment, the launchpad installs WebSphere Application Server Network Deployment, WebSphere Application Server Feature Pack for XML, WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature, and WebSphere Process Server.

This procedure assumes that you have one or more of the following products already installed:

- WebSphere Process Server, the WebSphere Process Server Client, or WebSphere Enterprise Service Bus, version 7.0.

- WebSphere Application Server or WebSphere Application Server Network Deployment, version 7.0.

Procedure

1. Start the launchpad application by navigating into the directory where you extracted the image and entering the following command:

   - `Linux` `UNIX` **On Linux and UNIX platforms:** *extract_directory*/`launchpad.sh`

- **On Windows platforms (from a command line):**
  `extract_directory\launchpad.exe`

2. In the left pane of the launchpad, click one of the following entries depending on whether you are a root/Administrator or nonroot/nonadministrative user:
   - If you are a root or an Administrator user, click **New installation**.
   - If you are a nonroot or a nonadministrative user, click **Nonadministrative or nonroot installation**.

3. In step 1, specify the location for the WebSphere Application Server Network Deployment installation and click **Install WebSphere Application Server**.

   Restriction: Windows IBM Installation Manager requires that its installation directory path be 80 characters or less. Thus, it is recommended that you keep your user ID to 20 characters or less.
   The launchpad application performs the following tasks:
   - Installs WebSphere Application Server Network Deployment into the directory you specify.

     Important: This process occurs silently and can take several minutes. Do *not* proceed until a message indicates a successful installation.
   - Imports WebSphere Application Server into Installation Manager automatically.

   Important: This process occurs silently and can take several minutes. Do *not* proceed until a message indicates a successful installation and import into Installation Manager. Instead of a success message, you might receive one of the following messages:
   - `WebSphere Application Server installation failed.` In this case, review the following log file to identify the cause:
     - Linux UNIX **On Linux and UNIX platforms:** `was_home/logs/install/log.txt`
     - Windows **On Windows platforms:** `was_home\logs\install\log.txt`

     If the `logs` directory does not exist on your system, the installation failed very early in the process. In this case, review the following log file:
     - Linux UNIX **On Linux and UNIX platforms:** `user_home/waslogs/log.txt`
     - Windows **On Windows platforms:** `user_home\waslogs\log.txt`
   - `WebSphere Application Server installation was successful,` but there were errors importing into Installation Manager. In this case, review the following log file to identify the cause:
     - Linux UNIX **On Linux and UNIX platforms:** `was_home/logs/launchpad_import.txt`
     - Windows **On Windows platforms:** `was_home\logs\launchpad_import.txt`

4. On the launchpad page, in step 2, click **Install WebSphere Process Server**. The launchpad application starts Installation Manager and its Install Packages wizard.

5. On the Install page of the Install Packages wizard, all recommended packages, including WebSphere Application Server Feature Pack for XML, WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the SDO feature, and WebSphere Process Server are preselected for installation. Click **Next**.

6. On the Install Packages wizard Licenses page, read through the license agreements and then select **I accept the terms in the license agreements**. Click **Next**. The licenses for the feature packs are also displayed in the panel. You accept for all the licenses.

7. On the Install Packages wizard Location page, **IBM WebSphere Application Server - ND_xxxxx** (where **xxxxx** is the date timestamp) and the **Use the existing package group** radio button are selected by default. Leave those selections as they are and click **Next**.

   Note: The Install Packages wizard displays a message if it detects any running processes. If you see this message, click **Cancel**, shut down the running processes, and begin the installation again.

8. The Install Packages wizard checks your operating system to make sure that it meets the prerequisites for installing WebSphere Process Server. The action you take depends on the results of the prerequisite check:

   • If the prerequisite check is successful (that is, a supported operating system is found), no message is displayed. The installation continues on to the Install Packages wizard Features page. Proceed to step 9.

   • If the prerequisite check is not successful (for example, a supported operating system is not at the minimum supported level), you see an error message and the installation stops. You must address the problem described in the message before you can install WebSphere Process Server.

   • 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 a warning. You can continue with the installation, but the installation or product operation might not succeed until you apply maintenance.

     If you see such a warning, go to the product support Web pages and 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.

9. On the Install Packages wizard Features page, accept the default selections and click **Next**.

   a. Optional: To install samples, expand **IBM WebSphere Process Server 7.0.0.0** and then **WebSphere Process Server**, and select the check box for **Sample applications**. If you choose not to install sample applications, you can install them later by following the instructions under "To install the samples or a default stand-alone development profile after installation".

   b. Optional: To install a default stand-alone development profile for WebSphere Process Server, expand **IBM WebSphere Process Server 7.0.0.0** and then **WebSphere Process Server**, and select the check box for **Stand-alone development WebSphere Process Server profile (qwps)**. To install a default stand-alone development profile for WebSphere Enterprise Service Bus, select the check box for **Stand-alone development WebSphere Enterprise Service Bus profile (qesb)**.

     The stand-alone development profile is a default development profile that comes with Business Rules Manager enabled. If you select to create a development profile, you are asked to supply your administrator security ID and password credentials. You cannot use a development profile in a production environment. If you choose not to install a default stand-alone development profile, you can install one later by following the instructions under "To install the samples or a default stand-alone development profile after installation".

10. Review the summary information. If the summary information is incorrect, click **Back** to change your selections.
11. Click **Install**. When the installation is complete, a page displays the status of the installation and which packages have been successfully installed.

    Important: This process can take several minutes. Do *not* proceed until this page appears.
12. To launch the Profile Management Tool, leave the **Profile Management Tool** radio button selected. Otherwise, select the radio button for **None**.
13. Click **Finish**.

Results

You have two installations of WebSphere Process Server coexisting on the same system.

What to do next

You must define a stand-alone server profile or a deployment manager profile in the Profile Management Tool or using the manageprofiles command-line utility. Only profiles created with the Profile Management Tool or manageprofiles command-line utility can be used in production. See the topics under "Creating profiles" on page 196 and "Augmenting profiles" on page 300 for more information.

Restriction:

If you created a stand-alone development profile during installation, remember that it does not work in a production environment. It is intended to help you gain familiarity with WebSphere Process Server without having to create a working production profile. You can start it from its First steps console by performing the following steps:
1. Open a command window.
2. Change to one of the following directories depending on your platform and on which type of profile you created:

    - `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/`profiles/qwps/firststeps/wbi`

    - `Windows` **On Windows platforms:** *install_root*\`profiles\qwps\firststeps\wbi`

    - `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root*/`profiles/qesb/firststeps/esb`

    - `Windows` **On Windows platforms:** *install_root*\`profiles\qesb\firststeps\esb`

3. Issue the firststeps command to start the console:

    - `Linux` `UNIX` **On Linux and UNIX platforms:** `./firststeps.sh`

    - `Windows` **On Windows platforms:** `firststeps.bat`

To install the samples or a default stand-alone development profile after installation:
If you chose not to install the samples or a default stand-alone development profile, you can do so later by performing the following steps:

1. Launch the Installation Manager manually.
2. Click **File > Preferences**.
3. In the Repositories Preferences page, click **Add Repository**.
4. In the Add Repository page, browse to the location of the following file, ensure that the check box beside **Search service repositories during installation and updates** is *not* selected, and then click **OK**.

   - `Linux` `UNIX` **On Linux and UNIX platforms:** *extract_directory*/`repository/repository.config`

   - `Windows` **On Windows platforms (from a command line):** *extract_directory*\repository\repository.config

5. Return to the first page of the Installation Manager.
6. Select **Modify**.
7. Follow the instructions on the Modify wizard pages to install the sample applications, or to create a stand-alone WebSphere Process Server or WebSphere Enterprise Service Bus profile.

Creating new WebSphere Process Server profiles to coexist with profiles of other WebSphere products

Use this procedure to create a WebSphere Process Server, version 7.0 profile to coexist with configuration instances or profiles of other WebSphere products. This procedure uses the Profile Management Tool graphical user interface (GUI).

Before you begin

Review the general prerequisites for creating or augmenting profiles in "Prerequisites for creating or augmenting profiles" on page 189, as well as those specific to "Creating profiles using the Profile Management Tool" on page 197 or "Augmenting profiles using the Profile Management Tool" on page 301.

About this task

An installation of WebSphere Process Server, version 7.0 can run on the same system at the same time as installations of one or more of the following supported products and versions:

- IBM WebSphere Process Server, versions 7.0, 6.2, 6.1.x, and 6.0.x
- IBM WebSphere Enterprise Service Bus, versions 7.0, 6.2, 6.1.x, and 6.0.x
- IBM WebSphere Application Server, versions 7.0, 6.1, 6.0.x, and 5.x
- IBM WebSphere Application Server Network Deployment, versions 7.0, 6.1, 6.0.x, and 5.x
- IBM WebSphere Business Integration Sever Foundation, version 5.x
- `Linux` `UNIX` `Windows` IBM WebSphere Application Server Enterprise, version 5.0.x

You must have an existing configuration instance or profile.

To create a new WebSphere Process Server profile, use the following procedure.

Procedure

1. Create the new WebSphere Process Server profile.

To do so, follow the procedure in "Creating profiles using the Profile Management Tool" on page 197 or "Augmenting profiles using the Profile Management Tool" on page 301.

When progressing through the Profile Management Tool, on the Port values assignment panel, verify that the ports specified for the new profile are unique and different than the ports assigned to the existing configuration instance.

2. If you created a stand-alone server profile or deployment manager profile, verify that it is operating correctly with the coexisting instance. To verify that the profile is operating properly, start it from its First steps console while the coexisting instance is running. If it starts successfully, the profile is operating properly.

Results

A new WebSphere Process Server profile exists.

Updating the software interactively

Install updates to software packages you installed using IBM Installation Manager.

Before you begin

By default, Internet access is required unless your repository preferences point to your local update site.

Each installed package has the location embedded for its default IBM update repository. For Installation Manager to search the IBM update repository locations for the installed packages, the preference **Search service repositories during installation and updates** on the Repositories preference page must be selected. This preference is selected by default.

For more information about Installation Manager, access the Installation Manager tool help and documentation in the Installation Manager Information Center.

About this task

You can use this procedure to update packages that you installed using IBM Installation Manager. If you installed WebSphere Process Server using the procedure in "Installing WebSphere Process Server interactively for the first time" on page 43, "Installing WebSphere Process Server interactively over an existing installation of WebSphere Application Server Network Deployment" on page 47, or "Silently installing WebSphere Process Server" on page 53, these packages include:

- WebSphere Process Server
- WebSphere Application Server Feature Pack for XML
- WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature

You *cannot* use this procedure to install updates on the underlying WebSphere Application Server Network Deployment installation. To update WebSphere Application Server Network Deployment, use the IBM WebSphere Update Installer tool. For instructions on how to use this tool, see Installing maintenance packages, interim fixes, fix packs, and refresh packs in the WebSphere Application Server Network Deployment information center.

Important: If you apply fix packs to the underlying WebSphere Application Server Network Deployment installation, you must reimport it into Installation Manager. You do not have to reimport if you only apply interim fixes.

Procedure

1. Close all programs that were installed using Installation Manager before updating.
2. Start Installation Manager. See "Starting IBM Installation Manager manually" on page 67 for more information.
3. From the Start page of the Installation Manager, click **Update**.
4. If IBM Installation Manager is not detected on your system or if an older version is already installed, then you must continue with the installation of

the latest release. Follow the on-screen instructions in the wizard to complete the installation of IBM Installation Manager.

5. In the Update Packages wizard, select the package group containing the product package you want to update or select the **Update all** check box, and then click **Next**. Installation Manager searches for updates in its repositories and the predefined update sites for the software you are updating. A progress indicator shows the search is taking place.

6. If updates for a package are found, then they are displayed in the **Updates** list on the Update Packages page below their corresponding package. Only the latest recommended updates are displayed by default. Click **Show all** to display all updates found for the available packages.

   a. To learn more about an update, click the update and review its description under **Details**.

   b. If additional information about the update is available, a **More info** link is included at the end of the description text. Click the link to display the information in a browser. Review this information before installing the update.

7. Select the updates that you want to install or click **Select Recommended** to restore the default selections, and click **Next**. Updates that have a dependency relationship are automatically selected and cleared together.

   Important: If there is a dependency on a WebSphere Application Server fix, a prerequisite check failure reports the WebSphere Application Server fix that is required. You must run the IBM WebSphere Update Installer tool to apply the WebSphere Application Server fix. After you apply the fix, click the **Recheck** button to verify that the prerequisite has been fulfilled and proceed.

8. On the Licenses page, read the license agreements for the selected updates. On the left side of the Licenses page, the list of licenses for the updates you selected is displayed; click each item to display the license agreement text. If you agree to the terms of all the license agreements, click **I accept the terms of the license agreements**. Then click **Next**.

9. On the Summary page, review your choices before installing the updates.

   a. If you want to change the choices you made on previous pages, click **Back**, and make your changes.

   b. When you are satisfied, click **Update** to download and install the updates. A progress indicator shows the percentage of the installation completed.

   Note: During the update process, Installation Manager might prompt you for the location of the repository for the base version of the package. If you installed the product from DVDs or other media, they must be available when you use the update feature.

10. Optional: When the update process completes, a message that confirms the success of the process is displayed near the top of the page. Click **View log file** to open the log file for the current session in a new window. You must close the Installation Log window to continue.

11. Click **Finish** to close the wizard.

12. Close Installation Manager.

Results

All available product updates known to Installation Manager are installed.

Updating the software silently

Silently install updates to software packages you installed using IBM Installation Manager.

Before you begin

By default, Internet access is required unless your repository preferences point to your local update site.

About this task

You can use this procedure to update packages that you installed using IBM Installation Manager. Each installed package has the location embedded for its default IBM update repository. If you installed WebSphere Process Server using the procedure in "Installing WebSphere Process Server interactively for the first time" on page 43, "Installing WebSphere Process Server interactively over an existing installation of WebSphere Application Server Network Deployment" on page 47, or "Silently installing WebSphere Process Server" on page 53, these packages include:

- WebSphere Process Server
- WebSphere Application Server Feature Pack for XML
- WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature

You *cannot* use this procedure to install updates on the underlying WebSphere Application Server Network Deployment installation. To update WebSphere Application Server Network Deployment, use the IBM WebSphere Update Installer tool. For instructions on how to use this tool, see Installing maintenance packages, interim fixes, fix packs, and refresh packs in the WebSphere Application Server Network Deployment information center.

Important: If you apply fix packs to the underlying WebSphere Application Server Network Deployment installation, you must reimport it into Installation Manager. You do not have to reimport if you only apply interim fixes.

Procedure

1. Close all programs that were installed using Installation Manager before updating.
2. On a command line, change to the eclipse subdirectory into which you installed Installation Manager.
3. Enter and run the following command, substituting your own location, optionally, for the log file:

   - `Linux` `UNIX` `./IBMIM --launcher.ini silent-install.ini -updateAll -log` *log file path and name*

   - `Windows` `IBMIMc.exe --launcher.ini silent-install.ini -updateAll -log` *log file path and name*

   This command updates all package groups installed by the Installation Manager.

   For more information about Installation Manager, access the Installation Manager tool help and documentation in the Installation Manager Information Center.

Important: On Windows systems, you cannot use the command IBMIM.exe to start silent updates. You must use the command IBMIMc.exe. Do not use the command IBMIMc on Linux and UNIX systems.

Results

All available product updates known to Installation Manager are installed.

Rolling back updates

Using the Roll back packages wizard, you can remove updates to a WebSphere Process Server installation and revert to a previous version.

Before you begin

During the rollback process, Installation Manager must access files from the earlier version of the package. By default, these files are stored on your system when you install a package. If the files are not available on your workstation, you must include the location of the repository from which you installed the previous version of the product in your Installation Manager preferences (**File > Preferences > Repository**). If you installed the product from DVDs or other media, they must be available when you use the rollback function.

About this task

Use the rollback function if you have applied an update to a product package, and decide later that you want to remove the update and revert to the earlier version of the product. When you use the rollback function, the Installation Manager uninstalls the updated resources, and reinstalls the resources from the previous version. You can only roll back one version level at a time.

When you roll back to an earlier version of a package, it is restored with same features that were associated with that version. Use the Modify Packages wizard to add and remove features. See "Modifying a product installation" on page 66 for more information.

You can use this procedure to remove packages that you installed using IBM Installation Manager on the following products:
* WebSphere Process Server
* WebSphere Application Server Feature Pack for XML
* WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature

You *cannot* use this procedure to remove packages on the underlying WebSphere Application Server Network Deployment installation. To remove updates to WebSphere Application Server Network Deployment, use the IBM WebSphere Update Installer tool. For instructions on how to use this tool, see Installing maintenance packages, interim fixes, fix packs, and refresh packs in the WebSphere Application Server Network Deployment information center.

Important: If you remove fix packs to the underlying WebSphere Application Server Network Deployment installation, you must reimport it into Installation Manager. You do not have to reimport if you only remove interim fixes.

For more information about Installation Manager, access the Installation Manager tool help and documentation in the Installation Manager Information Center.

Procedure

1. Close all programs that were installed using Installation Manager before rolling back.
2. Start Installation Manager. See "Starting IBM Installation Manager manually" on page 67 for more information.
3. From the Start page of the Installation Manager, click **Roll back** to start the Roll back packages wizard.
4. On the Roll Back Packages page, from the Package Group Name list, select the package group that contains the packages that you want to roll back and click **Next**.
5. Select the version of the package to which you want to roll back and click **Next**.
6. Read the summary information and click **Roll Back** to roll back the package.
7. Optional: When the rollback process completes, a message that confirms the success of the process is displayed near the top of the page. Click **View log file** to open the log file for the current session in a new window.
8. Click **Finish** to close the wizard.
9. Close Installation Manager.

Results

The package you selected to roll back is removed.

Uninstalling the software

You uninstall WebSphere Process Server using the Installation Manager. If you plan to reinstall WebSphere Process Server to the same directory, complete the manual steps to ensure that all files and registry entries are deleted.

Also covered is how to remove the different components from a WebSphere Process Server installation. These components are uninstalled during an uninstallation of WebSphere Process Server. See the topics under Removing the Business Process Choreographer configuration and Removing the Common Event Infrastructure configuration for more information.

To uninstall related products, such as the Web server plug-ins for WebSphere Application Server, IBM HTTP Server, and the Application Client for WebSphere Application Server, see the following topics in the WebSphere Application Server Network Deployment and IBM HTTP Server information centers:

- Uninstalling the Web server plug-ins for WebSphere Application Server
- Uninstalling IBM HTTP Server
- Uninstalling Application Client for WebSphere Application Server feature pack

Uninstalling WebSphere Process Server using Installation Manager

Uninstall WebSphere Process Server using the Installation Manager.

Before you begin

Close all programs that you installed using Installation Manager.

About this task

To uninstall the packages, you must log in to the system using the same user account that you used to install the product packages.

A package cannot be uninstalled when another package has a dependency on it, unless the dependent package is also selected to be uninstalled. For example, you can uninstall the WebSphere Application Server Network Deployment installation underlying WebSphere Process Server, as long as other products are not dependent on WebSphere Application Server Network Deployment.

Important: Use Installation Manager to uninstall the WebSphere Application Server Network Deployment installation underlying WebSphere Process Server. Do not use the ISMP-based uninstaller included with the product. Doing so corrupts your installation of Installation Manager.

For more information about Installation Manager, access the Installation Manager tool help and documentation in the Installation Manager Information Center.

Procedure
1. Launch Installation Manager.
2. Click **Uninstall**.
3. Select **IBM WebSphere Process Server** and click **Next**.

4. Review the summary information.
   - If the summary information is incorrect, click **Back** to change your selections.
   - If the summary information is correct for your installation, click **Uninstall**. You see a page with the status of the products that were uninstalled.
5. Click **Finish**.

Results

The uninstallation of WebSphere Process Server is complete.

Important: Do not delete the Eclipse configuration directory after uninstalling any package. Deleting this information will interfere with the operation of Installation Manager. By default, this is the `configuration` directory in the *install_root*.

Preparing for reinstallation after failed uninstallation

Learn how to reinstall the software. An uninstallation program that does not complete successfully can leave files that can prevent you from reinstalling into the original directory. This topic outlines the procedures you need to follow in order to reinstall WebSphere Process Server.

Before you begin

You can reinstall WebSphere Process Server without a clean system. However, such an installation creates a coexistence scenario that can prevent you from installing into the original directory.

Cleaning the system means deleting everything from the previous installation, including log files that are left behind by the uninstallation procedure. Before you start the procedure, back up log files, if necessary. See "Installation and profile creation log files" on page 145 for the location of log files.

About this task

Other related products might be part of your installation and need to be uninstalled. For instructions, see the following topics in the WebSphere Application Server Network Deployment and IBM HTTP Server, version 7.0 information centers:

- Uninstalling the Web server plug-ins for WebSphere Application Server
- `Linux` `UNIX` `Windows` Uninstalling IBM HTTP Server
- Uninstalling Application Client for WebSphere Application Server feature pack

To prepare for reinstallation after a failed uninstallation, follow the appropriate instructions in the subtopics below. Cleaning the system eliminates all evidence of a deleted installation. After you have cleaned your system, go to Installing the software for information on how to install the product again.

Preparing for reinstallation after failed uninstallation on AIX systems

Learn how to clean an AIX system if uninstallation of WebSphere Process Server fails. After running the uninstallation program, go through these manual steps to remove registry entries that can prevent you from reinstalling the product into the original directory.

Before you begin

Perform this procedure only if you attempted to uninstall WebSphere Process Server using the Installation Manager and that procedure was not completed successfully.

Note: If you successfully uninstalled WebSphere Process Server, you do not need to perform this task.

Determine the *install_root* directory for the product so that you remove the correct product and produce a clean system.

For details on default directory locations, see "Default installation directories for the product and profiles" on page 127.

Note:

The Installation Manager and the Profile Management Tool let you specify your own locations for installation root directories. Examine the following files to determine the actual locations:

- The `/usr/.ibm/.nif/.nifregistry` file identifies the installation root for all installed WebSphere Process Server products; it also looks for all WebSphere Application Server products.
- The `install_root/logs/manageprofiles/profile_name_create.log` file for each created profile identifies the installation location in the stanza with the invokeWSProfile method.

Uninstalling the product leaves the `profile_root` directory, including the `profile_root/logs` file, where `profile_root` represents the installation location of the profile. It leaves the `install_root/logs` directory as well.

About this task

Reinstalling the product into a new directory when files remain from a previous installation can create a coexistence scenario. However, you can delete all files and registry entries to completely remove WebSphere Process Server. A clean system lets you reinstall the product into the original directory without coexistence.

Important: This procedure describes how to remove artifacts left after uninstallation of both WebSphere Process Server and WebSphere Application Server or WebSphere Application Server Network Deployment. The WebSphere Application Server product addressed is assumed to be the one underlying the installation of WebSphere Process Server.

Perform the following procedure to produce a clean system.

Procedure

1. Log on as the same user ID who installed the product.
2. Use the **kill** command to stop all Java processes that are running.

   If you are running Java processes that are not related to WebSphere Process Server or WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Process Server and WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

   ```
   ps -ef | grep java
   ```

Stop all WebSphere Process Server and WebSphere Application Server product-related processes with the kill command:

```
kill -9 java_pid_1java_pid_2 ...java_pid_n
```

3. List WebSphere Process Server and WebSphere Application Server components that are installed.

   Type the following command to search for related packages:

   ```
   lslpp -l | grep -i WS
   ```

   To narrow your query to search for WebSphere Process Server packages only, type the following command:

   ```
   lslpp -l | grep -i WSEAA70
   ```

   WebSphere Process Server, version 7.0 package names have a prefix of WSE and a suffix of 70. WebSphere Application Server Network Deployment, version 7.0 package names have a prefix of WSB or WSP and a suffix of 70.

   Do not remove packages for WebSphere Process Server and WebSphere Application Server products that you did not uninstall.

4. Change to the /usr/IBM directory or the equivalent top directory of your installation.

5. Type rm -rf WebSphere to delete this WebSphere Process Server-related directory, but only if the ProcServer (or AppServer directory associated with the WebSphere Process Server installation you removed) is the only directory within the WebSphere directory. Delete the directory if the only products contained in the directory are products that you intend to delete.

6. Use the installRegistryUtils command to examine the installation locations for all installed WebSphere server products and remove the desired products from the installation registry.

7. Edit the vpd.properties file to remove the entries for WebSphere Application Server. Refer to the topic Manually uninstalling on AIX systems in the WebSphere Application Server Network Deployment information center for instructions.

8. Run the WPS_ODM_clean.sh script.

   a. Obtain the scripts from the technote document titled Manual Object Data Manager (ODM) cleanup script for AIX on the WebSphere Application Server Support site.

   b. Edit the WPS_ODM_clean.sh script and replace every instance of the string /usr/WebSphere/AppServer with the actual installation root directory.

   c. Run the WPS_ODM_clean.sh script from the command line.

9. Clean the nifregistry file. To clean this file:

   a. Back up the .nifregistry file.

   b. Open the .nifregistry file in a text editor. Ensure that line wrapping is turned off.

   c. Search and delete all lines that have the *<INSTALL_LOC>* and *<PRODUCT_ID>* in them, where *<INSTALL_LOC>* is the installation location where you have a failed uninstallation and *<PRODUCT_ID>* is the product offering ID of the product that you are trying to uninstall

   d. Save the .nifregistry file and close the text editor.

Results

This procedure results in a clean system. You can reinstall WebSphere Process Server into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

After you have cleaned your system, go to "Installing the software" on page 41 to choose an installation procedure.

Preparing for reinstallation after failed uninstallation on HP-UX systems

Learn how to clean an HP-UX system if uninstallation of WebSphere Process Server fails. After running the uninstallation program, go through these manual steps to remove registry entries that can prevent you from reinstalling the product into the original directory.

Before you begin

Perform this procedure only if you attempted to uninstall WebSphere Process Server using the Installation Manager and that procedure was not completed successfully.

Note: If you successfully uninstalled WebSphere Process Server, you do not need to perform this task.

Determine the *install_root* directory for the product so that you remove the correct product and produce a clean system.

For details on default directory locations, see "Default installation directories for the product and profiles" on page 127.

Note:

TheInstallation Manager and the Profile Management Tool let you specify your own locations for installation root directories. Examine the following files to determine the actual locations:

*   The `opt/.ibm/.nif/.nifregistry` file identifies the installation root for all installed WebSphere Process Server products; it also looks for all WebSphere Application Server products.
*   The `install_root/logs/manageprofiles/profile_name_create.log` file for each created profile identifies the installation location in the stanza with the invokeWSProfile method.

Uninstalling the product leaves the `profile_root` directory, including the `profile_root/logs` file, where `profile_root` represents the installation location of the profile. It leaves the `install_root/logs` directory as well.

About this task

Reinstalling the product into a new directory when files remain from a previous installation can create a coexistence scenario. However, you can delete all files and registry entries to completely remove WebSphere Process Server. A clean system lets you reinstall the product into the original directory without coexistence.

Important: This procedure describes how to remove artifacts left after uninstallation of bothWebSphere Process Server and WebSphere Application Server or WebSphere Application Server Network Deployment. The WebSphere Application Server product addressed is assumed to be the one underlying the installation of WebSphere Process Server.

Perform the following procedure to produce a clean system.

Procedure

1. Log on as the same user ID who installed the product.
2. Use the **kill** command to stop all Java processes that are running.

   If you are running Java processes that are not related to WebSphere Process Server or WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Process Server and WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

   ```
   ps -ef | grep java
   ```

   Stop all WebSphere Process Server and WebSphere Application Server product-related processes with the kill command:

   ```
   kill -9 java_pid_1java_pid_2 ...java_pid_n
   ```

3. Use the HP-UX System Administration Manager (SAM) utility to remove packages.
   a. Start the SAM utility with the `/usr/sbin/sam` command.
   b. Verify that your DISPLAY and TERM environment variables are set properly.
   c. Click **Software management**.
   d. Click **View installed software**.
   e. Look for WebSphere Process Server or WebSphere Application Server entries in the SD list.
   f. Close the SD list.
   g. Click **Remove local host software**.
   h. Select any of the following instances that are displayed in the SD Remove List:
      - **WSEAA70**
      - **WSBAA70**
   i. Select **Actions** → **Mark for remove**.
   j. Select **Actions** → **Remove**.
   k. Click **OK** in the Remove analysis dialog box.
   l. Click **Logs** to display real-time removal of selected packages.
   m. Click **Done** when all packages are removed.
   n. Exit SAM.

4. Search for the packages to verify their removal.

   Type `swlist | grep WS` to show packages for WebSphere Process Server and WebSphere Application Server.

   To narrow your query to search for WebSphere Process Server packages only, type the following command:

   ```
   swlist | grep WSEAA70
   ```

5. Remove the installation root directory.

   Type `rm -rf install_root` to remove WebSphere Process Server directories. Ensure you specify the correct *install_root* for the product you uninstalled.

   For example, if you uninstalled WebSphere Process Server from the default installation directory (`/opt/IBM/WebSphere/ProcServer`), issue the following command:

   ```
   rm -rf /opt/IBM/WebSphere/ProcServer
   ```

6. Use the installRegistryUtils command to examine the installation locations for all installed WebSphere server products and remove the desired products from the installation registry.

7. Clean the .nifregistry file. To clean this file:

    a. Back up the .nifregistry file.

    b. Open the .nifregistry file in a text editor. Ensure that line wrapping is turned off.

    c. Search and delete all lines that have the *<INSTALL_LOC>* and *<PRODUCT_ID>* in them, where *<INSTALL_LOC>* is the installation location where you have a failed uninstallation and *<PRODUCT_ID>* is the product offering ID of the product that you are trying to uninstall.

    d. Save the .nifregistry file and close the text editor.

Results

This procedure results in a clean system. You can reinstall WebSphere Process Server into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

After you have cleaned your system, go to "Installing the software" on page 41 to choose an installation procedure.

Preparing for reinstallation after failed uninstallation on Linux systems

Learn how to clean a Linux system if uninstallation of WebSphere Process Server fails. After running the uninstallation program, go through these manual steps to remove registry entries that can prevent you from reinstalling the product into the original directory.

Before you begin

Perform this procedure only if you attempted to uninstall WebSphere Process Server using the Installation Manager and that procedure was not completed successfully.

Note: If you successfully uninstalled WebSphere Process Server, you do not need to perform this task.

Determine the *install_root* directory for the product so that you remove the correct product and produce a clean system.

For details on default directory locations, see "Default installation directories for the product and profiles" on page 127.

Note:

The Installation Manager and the Profile Management Tool let you specify your own locations for installation root directories. Examine the following files to determine the actual locations:

- The `opt/.ibm/.nif/.nifregistry` file identifies the installation root for all installed WebSphere Process Server products; it also looks for all WebSphere Application Server products.

- The *install_root*/logs/manageprofiles/*profile_name*_create.log file for each created profile identifies the installation location in the stanza with the invokeWSProfile method.

Uninstalling the product leaves the *profile_root* directory, including the *profile_root*/logs file, where *profile_root* represents the installation location of the profile. It leaves the *install_root*/logs directory as well.

About this task

Reinstalling the product into a new directory when files remain from a previous installation can create a coexistence scenario. However, you can delete all files and registry entries to completely remove WebSphere Process Server. A clean system lets you reinstall the product into the original directory without coexistence.

Important: This procedure describes how to remove artifacts left after uninstallation of both WebSphere Process Server and WebSphere Application Server or WebSphere Application Server Network Deployment. The WebSphere Application Server product addressed is assumed to be the one underlying the installation of WebSphere Process Server.

Perform the following procedure to produce a clean system.

Procedure

1. Log on as the same user ID who installed the product.
2. Use the **kill** command to stop all Java processes that are running.

   If you are running Java processes that are not related to WebSphere Process Server or WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Process Server and WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

   ```
   ps -ef | grep java
   ```

   Stop all WebSphere Process Server and WebSphere Application Server product-related processes with the kill command:

   ```
   kill -9 java_pid_1java_pid_2 ...java_pid_n
   ```

3. Search for related packages. Issue the following command to show packages for the WebSphere Process Server and WebSphere Application Server products:

   ```
   rpm -qa | grep WS
   ```

   To narrow your query to search for WebSphere Process Server packages only, type the following command:

   ```
   rpm -qa | grep WSEAA70
   ```

   For example, after you issue the command rpm -qa | grep WSEAA70, the following package might be displayed:

   ```
   WSEAA70LicensingComponent-7.0-0
   ```

   WebSphere Process Server, version 7.0 package names have a prefix of WSE and a suffix of 70. WebSphere Application Server Network Deployment, version 7.0 package names have a prefix of WSB or WSP and a suffix of 70. Do not remove packages for WebSphere Process Server and WebSphere Application Server products that you did not uninstall.

4. If there are packages to delete, type rpm **-e** *packagename* to remove any packages for the product that you uninstalled.

Alternatively, you can search for packages to verify that every item in the list is something to delete:

```
rpm -qa | grep WSEAA70
```

If the list contains packages that you intend to delete and no others, remove all of the packages with the following command:

```
rpm -qa | grep WSEAA70 | xargs rpm -e
```

If there is a problem with package dependencies, you can use the following command to remove the packages:

```
rpm -e packagename --nodeps --justdb
```

The nodeps option skips the dependency check. The justdb option updates only the package database, and not the file system. Using only the nodeps option can cause a failure in package removal if there is any mismatch in the dependent file system (files and directories).

5. Remove the installation root directory.

   Type `rm -rf install_root` to remove WebSphere Process Server directories. Ensure you specify the correct *install_root* for the product you uninstalled.

   For example, if you uninstalled WebSphere Process Server from the default installation directory (`/opt/ibm/WebSphere/ProcServer`), issue the following command:

   ```
   rm -rf /opt/ibm/WebSphere/ProcServer
   ```

6. Edit the `vpd.properties` file to remove the entries for WebSphere Application Server. Refer to the topic Manually uninstalling on Linux systems in the WebSphere Application Server Network Deployment information center for instructions.

7. Edit the `/opt/.ibm/.nif/.nifRegistry` file.

   This file is located in the home directory of the user ID from which the product was installed.

   The `/opt/.ibm/.nif/.nifRegistry` file contains a one-line entry for each WebSphere Process Server product installation and also an entry for each WebSphere Application Server product installation.

   Use a flat-file editor to remove the line that identifies the installation root directory of the product that you removed. Leave the other lines intact.

8. Use the installRegistryUtils command to examine the installation locations for all installed WebSphere Process Server products and remove the desired products from the installation registry.

Results

This procedure results in a clean system. You can reinstall WebSphere Process Server into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

After you have cleaned your system, go to "Installing the software" on page 41 to choose an installation procedure.

Preparing for reinstallation after failed uninstallation on Solaris systems

Learn how to clean a Solaris system if uninstallation of WebSphere Process Server fails. After running the uninstallation program, go through these manual steps to remove registry entries that can prevent you from reinstalling the product into the original directory.

Before you begin

Perform this procedure only if you attempted to uninstall WebSphere Process Server using the Installation Manager and that procedure was not completed successfully.

Note: If you successfully uninstalled WebSphere Process Server, you do not need to perform this task.

Determine the *install_root* directory for the product so that you remove the correct product and produce a clean system.

For details on default directory locations, see "Default installation directories for the product and profiles" on page 127.

Note:

The Installation Manager and the Profile Management Tool let you specify your own locations for installation root directories. Examine the following files to determine the actual locations:

- The `opt/.ibm/.nif/.nifregistry` file identifies the installation root for all installed WebSphere Process Server products; it also looks for all WebSphere Application Server products.
- The `install_root`/logs/manageprofiles/`profile_name_`create.log file for each created profile identifies the installation location in the stanza with the invokeWSProfile method.

Uninstalling the product leaves the `profile_root` directory, including the `profile_root`/logs file, where `profile_root` represents the installation location of the profile. It leaves the `install_root`/logs directory as well.

About this task

Reinstalling the product into a new directory when files remain from a previous installation can create a coexistence scenario. However, you can delete all files and registry entries to completely remove WebSphere Process Server. A clean system lets you reinstall the product into the original directory without coexistence.

Important: This procedure describes how to remove artifacts left after uninstallation of bothWebSphere Process Server and WebSphere Application Server or WebSphere Application Server Network Deployment. The WebSphere Application Server product addressed is assumed to be the one underlying the installation of WebSphere Process Server.

Perform the following procedure to produce a clean system.

Procedure

1. Log on as the same user ID who installed the product.

2. Use the **kill** command to stop all Java processes that are running.

   If you are running Java processes that are not related to WebSphere Process Server or WebSphere Application Server products and it is not possible to stop them, stop all WebSphere Process Server and WebSphere Application Server product-related processes. Use the following command to determine all processes that are running:

   ```
   ps -ef | grep java
   ```

   Stop all WebSphere Process Server and WebSphere Application Server product-related processes with the kill command:

   ```
   kill -9 java_pid_1java_pid_2 ...java_pid_n
   ```

3. Search for related packages. Issue the following command to show packages for the WebSphere Process Server and WebSphere Application Server products (if no packages appear when using these commands, skip the next step):

   ```
   pkginfo | grep WS
   ```

   To narrow your query to search for WebSphere Process Server packages only, type the following command:

   ```
   pkginfo | grep WSEAA70
   ```

   For example, after you issue the command `pkginfo | grep WSEAA70`, the following list of packages might be displayed:

   ```
   application WSEAA70                          IBM WebSphere Process Server
   application WSEAA70LC                        LAP Component
   ```

   WebSphere Process Server, version 7.0 package names have a prefix of WSE and a suffix of 70. WebSphere Application Server Network Deployment, version 7.0 package names have a prefix of WSB or WSP and a suffix of 70.

   Do not remove packages for WebSphere Process Server and WebSphere Application Server products that you did not uninstall.

4. Change to the directory where package information is registered.

   ```
   cd /var/sadm/pkg
   ```

5. Issue the following command to remove any WebSphere Process Server or WebSphere Application Server product-related packages.

   ```
   pkgrm packagename1 packagename2 packagename3 ...
   ```

   Do not remove packages for WebSphere Process Server and WebSphere Application Server products that you did not uninstall.

   Issue the following commands from the /var/sadm/pkg directory to search for and remove any WebSphere Application Server product-related packages that are registered in the /var/sadm/pkg directory:

   a. Change to the correct directory: `cd /var/sadm/pkg`

   b. `ls |grep WSB|xargs -i pkgrm -n {}` for WebSphere Application Server products

   c. `ls |grep WSC|xargs -i pkgrm -n {}` for WebSphere Application Server Clients

   d. `ls |grep WSP|xargs -i pkgrm -n {}` for Web server plug-ins for WebSphere Application Server

   e. `ls |grep WSE|xargs -i pkgrm -n {}` for WebSphere Process Server

   Package names for Web server plug-ins for WebSphere Application Server are:

   ```
   WSPAA70
   WSPAA70AC
   WSPAA70BC
   WSPAA70CC
   ```

```
WSPAA70DC
WSPAA70FC
WSPAA70FB
WSPAA70GC
WSPAA70HC
```

If there is a problem removing the packages, remove the related package directories in the `/var/sadm/pkg` directory, including the preremove files. For example, remove the following file before issuing the pkgrm -n WSBAA70 command:

`/var/sadm/pkg/WSBAA70/install/preremove`

6. Remove any profile directories that are not located in the installation root (*install_root*) directory.

   To determine the locations of profile directories, first use the `wasprofile -listProfiles` command to display profile names. Then, to determine where profile directories are located, use the `wasprofile -getPath -profileName` *profile_name* command, where *profile_name* is the name of the profile corresponding to a given directory.

7. Remove the installation root directory. Type `rm -rf` *install_root* to remove WebSphere Process Server directories. Ensure you specify the correct *install_root* for the product you uninstalled. For example, if you uninstalled WebSphere Process Server from the default installation directory `/opt/IBM/WebSphere/ProcServer`, issue the following command:

   `rm -rf /opt/IBM/WebSphere/ProcServer`

   Remove all of the profile directories as well.

8. Edit the `/opt/.ibm/.nif/.nifregistry` file.

   This file contains a one-line entry for each WebSphere Process Server product installation and has an entry for each WebSphere Application Server product installation.

   You can delete these files if there is just one line in each that identifies the product that you removed. Otherwise, use a flat-file editor to remove the line that identifies the installation root directory of the product that you removed. Leave the other lines intact.

9. Use the installRegistryUtils command to examine the installation locations for all installed WebSphere Process Server products and remove the desired products from the installation registry.

Results

This procedure results in a clean system. You can reinstall WebSphere Process Server into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

After you have cleaned your system, go to "Installing the software" on page 41 to choose an installation procedure.

Preparing for reinstallation after a failed uninstallation on Windows systems

Learn how to clean a Windows system if uninstallation of WebSphere Process Server fails. After running the uninstallation program, go through these manual steps to remove registry entries that can prevent you from reinstalling the product into the original directory.

Before you begin

Before performing this procedure, ensure you have uninstalled WebSphere Process Server and that procedure was not completed successfully. If the procedure was successful, you do not need to perform this task.

Determine the *install_root* directory for the product so that you remove the correct product and produce a clean system.

For details on default directory locations, see "Default installation directories for the product and profiles" on page 127.

Examine the following files to determine the actual location for the installation root directories.

- The `.nifRegistry` file identifies the installation root for all installed WebSphere Process Server products; it also identifies the installation root for all installed WebSphere Application Server products. It is located as follows:
  - If the user ID that installed the product had administrative privileges, the file is located in the Windows root directory (`C:\Windows` or `C:\WINNT` on most Windows systems).
  - If the user ID that installed the product did not have administrative privileges, the file is located in the home directory of that user ID.
- The `install_root\logs\manageprofiles\`*profile_name*`_create.log` file for a profile identifies the location of that profile. Search on the text `profilePath=` in this file to obtain the location of the profile.

Uninstalling the product leaves the *profile_root* directory, including the `profile_root\logs` directory, where *profile_root* represents the installation location of the profile. It leaves the `install_root\logs` directory as well.

About this task

Reinstalling the product into a new directory when files remain from a previous installation can create a coexistence scenario. However, you can delete all files and registry entries to completely remove WebSphere Process Server. A clean system lets you reinstall the product into the original directory without coexistence.

Important: This procedure describes how to remove artifacts left after uninstallation of both WebSphere Process Server and WebSphere Application Server or WebSphere Application Server Network Deployment. The WebSphere Application Server product addressed is assumed to be the one underlying the installation of WebSphere Process Server.

Perform the following procedure to produce a clean system.

Procedure

1. Log on as the same user ID who installed the product.
2. Optional: Verify that you have an Emergency Recovery Disk. Instructions for creating this disk are in the Windows help documentation.

   This step is a safeguard. This procedure does not require the recovery disk.
3. Optional: Use the regback.exe program from the Windows Resource Kit to back up the registry.

   This step is a safeguard. This procedure does not require the backup copy of the registry.

4. Delete product registry entries for the WebSphere Process Server and WebSphere Application Server products that you uninstalled.

   Invoke regback.exe from a command prompt to edit the Windows system registry.

   CAUTION:

   Handle the Registry with care. You can easily make a mistake while using the registry editor to view and edit registry contents. The editor does not warn you of editing errors, which can be extremely dangerous. A corrupt registry can disrupt your system to the point where your only option is to reinstall the Windows operating system.

   a. Use **Ctrl-F** to search for all instances of "WebSphere," to determine whether you should delete each entry. You might not be able to remove all of the entries related to WebSphere Process Server and WebSphere Application Server, which is not a problem.

   b. Expand and select keys related to WebSphere Process Server and WebSphere Application Server products.

      Delete the following keys if present for the WebSphere Application Server product:

      - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\`
        `Explorer\MenuOrder\Start Menu2\Programs\IBM WebSphere\Application`
        `Server Network Deployment V7.0`

      - `HKEY_CURRENT_USER\Software\IBM\WebSphere Application Server`
        `Network Deployment\7.0.0.0`

      - `HKEY_LOCAL_MACHINE\Software\IBM\Web server Plug-ins for IBM`
        `WebSphere Application Server\7.0.0.0`

      Delete the following keys if present for the WebSphere Process Server product:

      - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\`
        `Explorer\MenuOrder\Start Menu2\Programs\IBM WebSphere\Process`
        `Server 7.0`

      - `HKEY_CURRENT_USER\Software\IBM\WebSphere Process Server\7.0`

   c. Select **Edit > Delete** from the menu bar for each related key.

   d. Select **Yes** when asked to confirm deletion of the key.

   e. Select **Registry > Exit** from the menu bar when you are finished.

5. Delete the installation root directory for the product that you uninstalled.

6. Using regedit, delete any registry keys of the form `HKEY_LOCAL_MACHINE\`
   `SYSTEM\CurrentControlSet\Services\IBMWAS61Service` that are associated with the installation you uninstalled.

7. Determine all the profile directories, and remove the directories.

8. Open a Windows Explorer window and browse to the following directory (where *user_id* is the user who installed the product): `C:\Documents and`
   `Settings\`*`user_id`*`\Start Menu\Programs\IBM WebSphere`

   If you have only one installation of WebSphere Application Server, delete the following folder if present:

   `Application Server V7.0`

   If you have only one installation of WebSphere Application Server Network Deployment, delete the following folder if it is present:

   `Application Server Network Deployment V7.0`

   If you have only one installation of WebSphere Process Server, delete the following folder if it is present:

```
Process Server 7.0
```

If you have multiple versions of WebSphere Application Server or WebSphere Process Server installed, the folder names will be appended with a number, as in the following examples:

- `Application Server Network Deployment V7.0 (2)`
- `Process Server 7.0 (2)`

In this case, you can use the following procedure to determine which folder or folders to delete:

a. In Windows Explorer, open `C:\Documents and Settings\`*user_id*`\Start Menu\Programs\IBM WebSphere\` (where *user_id* is the user who installed the product).

b. Open the `Application Server V7.0` or `Application Server Network Deployment V7.0` folder.

c. Right-click the `Profile Management Tool` subfolder and select **Properties**. Then select the **Shortcut** tab.

d. Examine the **Target** property and determine if the Target directory points to the WebSphere Application Server installation that failed to uninstall. If that is the case, delete the `Application Server V7.0` or `Application Server Network Deployment V7.0` folder.

e. Repeat steps b through d, but this time for step b start with the `Process Server 7.0` subfolder, and, for step d, determine if the Target directory points to the WebSphere Process Server installation that failed to uninstall.

f. Repeat steps b through e for each additional set of folders (for example, `Application Server Network Deployment V7.0 (2)` and `Process Server 7.0 (2)`.

9. Edit your entries in the `.nifRegistry` file.

   The `.nifRegistry` file is located as follows:

   - If the user ID that installed the product had administrative privileges, the file is located in the Windows root directory (`C:\Windows` or `C:\WINNT` on most Windows systems).
   - If the user ID that installed the product did not have administrative privileges, the file is located in the home directory of that user ID.

   The `.nifRegistry` file contains a one-line entry for each WebSphere Process Server product installation and each WebSphere Application Server product installation.

   You can delete this file if there is just one line that identifies the product that you removed. Otherwise, use a flat-file editor to remove the line that identifies the installation root directory of the product that you removed. Leave the other lines intact. Do not delete the `.nifRegistry` file unless you removed all of the installations listed in the file.

10. Use the installRegistryUtils command to examine the installation locations for all installed WebSphere server products and remove the desired products from the installation registry.

11. Restart your server if a prompt is displayed that directs you to restart.

Results

This procedure results in a clean system. You can reinstall WebSphere Process Server into the same directories now. A clean system has no trace of a previously deleted installation.

What to do next

After you have cleaned your system, go to "Installing the software" on page 41 to choose an installation procedure.

Uninstalling Business Process Choreographer

For information on how to remove Business Process Choreographer from a WebSphere Process Server installation, go to the WebSphere Process Server for Multiplatforms, version 7.0, information center and review the topics under **Installing WebSphere Process Server > Uninstalling the software > Removing the Business Process Choreographer configuration**. You can also find this information in the *Business Process Choreographer PDF*.

Installation information

This reference section contains subtasks and supporting conceptual and reference information related to installing WebSphere Process Server.

Default installation directories for the product and profiles

This topic discusses specific variables used within a WebSphere Process Server installation.

How variable meanings can differ

References in product information to *install_root* and *profile_root* represent specific default directory locations for the product installation and profile configuration files. This topic describes the conventions in use for WebSphere Process Server. The meaning of these variables can differ based on whether you are installing the product on a clean server or on one with an existing installation of WebSphere Application Server or WebSphere Application Server Network Deployment. They can also differ depending on whether you are performing the installation as a root (Administrator on a Windows system) or nonroot user.

Limitations of nonroot installers

`Linux` `UNIX` `Windows` Root, Administrator, and nonroot users can install the product. The default directories the installation program provides differ based on whether the user has root (Administrator) privileges. Root and Administrator users can register shared products and install into system-owned directories (globally shared resources that are available to all users), while nonroot users cannot. Nonroot users can install only into directories they own.

Variables used in the documentation

Several variables representing specific default directories are used throughout the documentation. These file paths are default locations. You can install the product and other components and create profiles in any directory for which you have write access. Multiple installations of WebSphere Process Server products or components require multiple locations.

Here are the main variables used in the documentation:

`Linux` `UNIX` `Windows` *install_root*
    Installation location of WebSphere Process Server. WebSphere Process Server is always installed in the same location as the WebSphere Application Server Network Deployment installation with which it is associated.

profile_root
    Location of a WebSphere Process Server profile.

Default directories on a clean server

The following tables show the default installation locations of the WebSphere Process Server base installation and its profiles when there is *not* an existing installation of any other WebSphere product.

Table 28 shows the default installation root directory into which the installation program installs both WebSphere Process Server and WebSphere Application Server Network Deployment for both root (Administrator) and nonroot users.

Table 28. install_root default directory

Default *install_root* for root or Administrator users	Default *install_root* for nonroot users
`AIX` /usr/IBM/WebSphere/ProcServer	`AIX` user_home/IBM/WebSphere/ProcServer
`HP-UX` `Solaris` /opt/IBM/WebSphere/ProcServer	`HP-UX` `Solaris` user_home/IBM/WebSphere/ProcServer
`Linux` /opt/ibm/WebSphere/ProcServer	`Linux` user_home/ibm/WebSphere/ProcServer
`Windows` C:\Program Files\IBM\WebSphere\ProcServer	`Windows` C:\IBM\WebSphere\ProcServer `Windows 7` c:\program files\IBM\WebSphere\ProcServer

Table 29 shows the default installation directory for a profile named *profile_name* for both root (Administrator) and nonroot users.

Table 29. profile_root default directory

Default *profile_root* for root or Administrator users	Default *profile_root* for nonroot users
`AIX` /usr/IBM/WebSphere/ProcServer/profiles/*profile_name*	`AIX` user_home/IBM/WebSphere/ProcServer/profiles/*profile_name*
`HP-UX` `Solaris` /opt/IBM/WebSphere/ProcServer/profiles/*profile_name*	`HP-UX` `Solaris` user_home/IBM/WebSphere/ProcServer/profiles/*profile_name*
`Linux` /opt/ibm/WebSphere/ProcServer/profiles/*profile_name*	`Linux` user_home/ibm/WebSphere/ProcServer/profiles/*profile_name*
`Windows` C:\Program Files\IBM\WebSphere\ProcServer\profiles*profile_name*	`Windows` C:\IBM\WebSphere\ProcServer\profiles*profile_name*

Default directories when an installation of WebSphere Application Server or WebSphere Application Server Network Deployment exists

When an installation of a supported version of WebSphere Application Server or WebSphere Application Server Network Deployment exists on a server and you elect to install WebSphere Process Server on top of it, WebSphere Process Server is installed into the same location. Table 30 on page 129 shows the default installation root directory in such a case for both root (Administrator) and nonroot users.

Table 30. install_root default directory when an existing installation of WebSphere Application Server or WebSphere Application Server Network Deployment exists

Default *install_root* for root or Administrator users	Default *install_root* for nonroot users
AIX `/usr/IBM/WebSphere/AppServer`	AIX *user_home*`/IBM/WebSphere/ AppServer`
HP-UX Linux Solaris `/opt/IBM/WebSphere/AppServer`	HP-UX Linux Solaris *user_home*`/IBM/WebSphere/AppServer`
Windows `C:\Program Files\IBM\ WebSphere\AppServer`	Windows `C:\IBM\WebSphere\AppServer`

The default directory for *profile_root* is handled similarly.

Default installation directories for Installation Manager

Table 31 shows two default directories related to the Installation Manager tool.

The directories under **Installation directory** are the defaults (per platform) into which the launchpad application installs Installation Manager.

The directories under **Agent data location directory** are the defaults (per platform) used by Installation Manager for data associated with the application, such as the state and history of operations performed by Installation Manager.

Values are given for both root (Administrator) and nonroot users.

For more information about the Agent data location, see Agent data location in the Installation Manager documentation. For more information on other defaults for Installation Manager, see Installing as an administrator or non-administrator in the Installation Manager documentation.

Table 31. Installation Manager default installation directories

Defaults for root or Administrator users	Defaults for nonroot users
Installation directory:	**Installation directory:**
Linux `/opt/IBM/InstallationManager/ eclipse`	Linux *user_home*`/IBM/ InstallationManager/eclipse`
UNIX `/opt/IBM/InstallationManager/ eclipse`	UNIX *user_home*`/IBM/ InstallationManager/eclipse`
Windows `C:\Program Files\IBM\ Installation Manager\eclipse`	Windows `C:\Documents and Settings\`*userID*`\IBM\Installation Manager\eclipse` Vista Windows 7 `C:\ProgramData\IBM\Installation Manager`
Agent data location directory:	**Agent data location directory:**
Linux `/var/ibm/InstallationManager`	Linux *user_home*`/var/ibm/ InstallationManager`
UNIX `/var/ibm/InstallationManager`	UNIX *user_home*`/var/ibm/ InstallationManager`

Table 31. Installation Manager default installation directories (continued)

Defaults for root or Administrator users	Defaults for nonroot users
Windows `C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager` **2008** **Vista** **Windows 7** `C:\ProgramData\IBM\Installation Manager`	**Windows** `C:\Documents and Settings\`*userID*`\Application Data\IBM\Installation Manager` **2008** **Vista** **Windows 7** `C:\Users\`*userID*`\AppData\Roaming\IBM\ Installation Manager`

installation commands

A summary of the commands used to install WebSphere Process Server and supporting products.

WebSphere Process Server product DVD

The product DVD includes the following products:
- WebSphere Process Server
- WebSphere Application Server Network Deployment
- WebSphere Application Server Feature Pack for XML
- WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature
- Installation Manager
- IBM WebSphere Process Server Help System

Table 32 lists the commands you use to silently install WebSphere Process Server. During product installation, the software also installs WebSphere Application Server Network Deployment, WebSphere Application Server Feature Pack for XML, WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature, and Installation Manager. You can also install WebSphere Process Server from the product launchpad.

The IBM WebSphere Process Server Help System must be installed from the product launchpad.

Table 32. Installation commands for WebSphere Process Server

Operating system	WebSphere Process Server
AIX	/responsefiles/wbi/run_templates (This is a silent installation that requires a response file. See "Silently installing WebSphere Process Server" on page 53 for details.)
HP-UX	/responsefiles/wbi/run_templates (This is a silent installation that requires a response file. See "Silently installing WebSphere Process Server" on page 53 for details.)
Linux	/responsefiles/wbi/run_templates (This is a silent installation that requires a response file. See "Silently installing WebSphere Process Server" on page 53 for details.)
Solaris	/responsefiles/wbi/run_templates (This is a silent installation that requires a response file. See "Silently installing WebSphere Process Server" on page 53 for details.)
Windows	\responsefiles\wbi\run_template.bat (This is a silent installation that requires a response file. See "Silently installing WebSphere Process Server" on page 53 for details.)

WebSphere Application Server Network Deployment Supplements V7.0 CDs

Table 33 lists the commands you use to install software supplied on the WebSphere Application Server Network Deployment Supplements V7.0 CDs. Except for IBM Support Assistant, you can also install these products from the WebSphere Process Server launchpad.

Table 33. Installation commands for software on WebSphere Application Server Network Deployment Supplements V7.0 CDs

Operating system	Application Client	IBM HTTP Server	Web Server Plug-ins	IBM Support Assistant
AIX	/AppClient/install	/IHS/install	/plugin/install	/ISA/install.bin
HP-UX	/AppClient/install	/IHS/install	/plugin/install	/ISA/install.bin
Linux	/AppClient/install	/IHS/install	/plugin/install	/ISA/install.bin
Solaris	/AppClient/install	/IHS/install	/plugin/install	/ISA/install.bin
Windows	\AppClient\install.exe	\IHS\install.exe	\plugin\install.exe	\ISA\install.exe

WebSphere Portal add-in for WebSphere Process Server V7.0 DVD

Table 34 lists the commands you use to install software supplied on the WebSphere Portal add-in for WebSphere Process Server V7.0 DVD. You can also install this add-in from the WebSphere Process Server launchpad.

Table 34. Installation commands for WebSphere Portal add-in for WebSphere Process Server V7.0 DVD

Operating system	WebSphere Portal add-in for WebSphere Process Server
AIX	/BSPACEP/install
HP-UX	/BSPACEP/install
Linux	/BSPACEP/install
Solaris	/BSPACEP/install
Windows	\BSPACEP\install.exe

Naming considerations for profiles, nodes, servers, hosts, and cells

This topic discusses reserved terms and issues you must consider when naming your profile, node, server, host and cell (if applicable).

Profile naming considerations

The profile name can be any unique name with the following restrictions. Do not use any of the following characters when naming your profile:

- Spaces
- Special characters that are not allowed within the name of a directory on your operating system, such as *, &, or ?.
- Slashes (/) or back slashes (\)

Double-byte characters are allowed.

Node, server, host, and cell naming considerations

Reserved names: Avoid using reserved folder names as field values. The use of reserved folder names can cause unpredictable results. The following words are reserved:

- cells
- nodes
- servers
- clusters
- applications
- deployments

Descriptions of fields on the Node and Hosts Names and Node, Host, and Cell Names pages: Table 35 describes the fields found on the Node and Host Names and Node, Host, and Cell Names pages of the Profile Management Tool, including the field names, default values, and constraints. Use this information as a guide when you are creating profiles.

Table 35. Naming guidelines for nodes, servers, hosts, and cells

Field name	Default value	Constraints	Description
Stand-alone server profiles			
Node name	Linux UNIX Windows *shortHostName* Node *NodeNumber* where: • *shortHost Name* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Avoid using the reserved names.	Select any name you want. To help organize your installation, use a unique name if you plan to create more than one server on the system.
Server name	Linux UNIX Windows server1	Use a unique name for the server.	The logical name for the server.
Host name	Linux UNIX Windows The long form of the domain name server (DNS) name.	The host name must be addressable through your network. If you are planning to use Business Space, use a fully qualified host name.	Use the actual DNS name or IP address of your workstation to enable communication with it. See additional information about the host name following this table.

Table 35. Naming guidelines for nodes, servers, hosts, and cells (continued)

Field name	Default value	Constraints	Description
Cell name	**Linux** **UNIX** **Windows** *shortHostName* Node *NodeNumber* Cell where: • *shortHost Name* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Use a unique name for the cell. A cell name must be unique in any circumstance in which the product is running on the same physical workstation or cluster of workstations, such as a Sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names also must be unique if their name spaces are going to be federated. Otherwise, you might encounter symptoms such as a javax.naming.Name NotFoundException exception, in which case, you need to create uniquely named cells.	All federated nodes become members of a deployment manager cell.
Deployment manager profiles			

Table 35. Naming guidelines for nodes, servers, hosts, and cells (continued)

Field name	Default value	Constraints	Description
Node name	**Linux** **UNIX** **Windows** *shortHostName* Cell Manager*Node Number* where: • *shortHost Name* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Use a unique name for the deployment manager. Avoid using the reserved names.	The name is used for administration within the deployment manager cell.
Host name	**Linux** **UNIX** **Windows** The long form of the domain name server (DNS) name.	The host name must be addressable through your network. Avoid using the reserved names. If you are planning to use Business Space, use a fully qualified host name.	Use the actual DNS name or IP address of your workstation to enable communication with it. See additional information about the host name following this table.

Table 35. Naming guidelines for nodes, servers, hosts, and cells (continued)

Field name	Default value	Constraints	Description
Cell name	Linux UNIX Windows *shortHostName* Cell *CellNumber* where: • *shortHost Name* is the short host name. • *CellNumber* is a sequential number starting at 01.	Use a unique name for the deployment manager cell. A cell name must be unique in any circumstance in which the product is running on the same physical workstation or cluster of workstations, such as a Sysplex. Additionally, a cell name must be unique in any circumstance in which network connectivity between entities is required either between the cells or from a client that must communicate with each of the cells. Cell names also must be unique if their name spaces are going to be federated. Otherwise, you might encounter symptoms such as a javax.naming.Name NotFoundException exception, in which case, you need to create uniquely named cells.	All federated nodes become members of the deployment manager cell , which you name in the Node, Host, and Cell Names page of the Profile Management Tool.
Custom profiles			

Table 35. Naming guidelines for nodes, servers, hosts, and cells (continued)

Field name	Default value	Constraints	Description
Node name	Linux UNIX Windows *shortHostName* Node *NodeNumber* where: • *shortHost Name* is the short host name. • *NodeNumber* is a sequential number starting at 01.	Avoid using the reserved names. Use a unique name within the deployment manager cell.	The name is used for administration within the deployment manager cell to which the custom profile is added. Use a unique name within the deployment manager cell.
Host name	Linux UNIX Windows The long form of the domain name server (DNS) name.	The host name must be addressable through your network. If you are planning to use Business Space, use a fully qualified host name.	Use the actual DNS name or IP address of your workstation to enable communication with it. See additional information about the host name following this table.

Windows **Directory path considerations:** The installation directory path must be less than or equal to 60 characters. The number of characters in the *profiles_directory_path\profile_name* directory must be less than or equal to 80 characters.

Host name considerations:

The host name is the network name for the physical workstation on which the node is installed. The host name must resolve to a physical network node on the server. When multiple network cards exist in the server, the host name or IP address must resolve to one of the network cards. Remote nodes use the host name to connect to and to communicate with this node.

WebSphere Process Server is compliant to both Internet Protocol version 4 (IPv4) and version 6 (IPv6). Wherever you can enter IP addresses in the administrative console, or elsewhere, you can do so in either format. Note that if IPv6 is implemented on your system you must enter the IP address in IPv6 format, and conversely, if IPv6 is not yet available to you, enter IP addresses in IPv4 format. For more information on IPv6 see the Official IPv6 Web site.

The following guidelines can help in determining the appropriate host name for your workstation:
• Select a host name that other workstations can reach within your network.
• Do not use the generic identifier, localhost, for this value.

- Do not attempt to install WebSphere Process Server products on a server with a host name that uses characters from the double-byte character set (DBCS). DBCS characters are not supported when used in the host name.
- Avoid using the underscore (_) character in server names. Internet standards dictate that domain names conform to the host name requirements described in Internet Official Protocol Standards RFC 952 and RFC 1123. Domain names must contain only letters (upper or lower case) and digits. Domain names can also contain dash characters (-) as long as the dashes are not on the ends of the name. Underscore characters (_) are not supported in the host name. If you have installed WebSphere Process Server on a server with an underscore character in the server name, access the server with its IP address until you rename it.

If you define coexisting nodes on the same computer with unique IP addresses, define each IP address in a domain name server (DNS) look-up table. Configuration files for servers do not provide domain name resolution for multiple IP addresses on a workstation with a single network address.

The value that you specify for the host name is used as the value of the hostName property in configuration documents. Specify the host name value in one of the following formats:
- Fully qualified domain name servers (DNS) host name string, such as xmachine.manhattan.ibm.com
- The default short DNS host name string, such as xmachine
- Numeric IP address, such as 127.1.255.3

The fully qualified DNS host name has the advantages of being totally unambiguous and flexible. You have the flexibility of changing the actual IP address for the host system without having to change the server configuration. This value for host name is particularly useful if you plan to change the IP address frequently when using Dynamic Host Configuration Protocol (DHCP) to assign IP addresses. A disadvantage of this format is being dependent on DNS. If DNS is not available, then connectivity is compromised.

The short host name is also dynamically resolvable. A short name format has the added ability of being redefined in the local hosts file so that the system can run the server even when disconnected from the network. Define the short name to 127.0.0.1 (local loopback) in the hosts file to run disconnected. A disadvantage of the short name format is being dependent on DNS for remote access. If DNS is not available, then connectivity is compromised.

A numeric IP address has the advantage of not requiring name resolution through DNS. A remote node can connect to the node you name with a numeric IP address without DNS being available. A disadvantage of this format is that the numeric IP address is fixed. You must change the setting of the hostName property in configuration documents whenever you change the workstation IP address. Therefore, do not use a numeric IP address if you use DHCP, or if you change IP addresses regularly. Another disadvantage of this format is that you cannot use the node if the host is disconnected from the network.

Related concepts

"Creating a Network Deployment configuration" on page 156
Creating a network deployment configuration involves installing WebSphere
Process Server, creating the appropriate profiles and configuring the deployment
environment.

WebSphere Process Server features

This topic describes the WebSphere Process Server features available for installation
in the Installation Manager.

Sample Applications

Selecting the WebSphere Process Server **Sample Applications** feature in Installation
Manager determines whether the sample applications for both WebSphere Process
Server and WebSphere Application Server Network Deployment are included in
your installation. Sample applications include both source code files and integrated
enterprise applications that demonstrate some of the latest Java Platform,
Enterprise Edition (Java EE) and WebSphere technologies.

For more information about sample applications, see Installing and accessing the
Samples Gallery.

For better performance in a production environment, do not install the Sample
Applications.

WebSphere Process Server - Client

Selecting **WebSphere Process Server - Client** on the features panel installs the
WebSphere Process Server Client and WebSphere Process Server. To install just the
WebSphere Process Server Client, clear the check box for WebSphere Process
Server.

Stand-alone WebSphere Process Server or WebSphere Enterprise Service Bus development profile

The Installation Manager includes an optional feature to create stand-alone
development profiles for both WebSphere Process Server and WebSphere
Enterprise Service Bus. These profiles will not work in a production environment.
They are intended for users to gain familiarity with WebSphere Process Server or
WebSphere Enterprise Service Bus without having to create working production
profiles. Creating these profiles requires you to supply your administrator security
ID and password credentials.

Product version and history information

Information and links to product version and history information.

The WBI.product file in the properties/version directory contains information such
as product, version, build date, and build level. For example:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE product SYSTEM "product.dtd">
<product name="IBM WebSphere Process Server">
```

```
<id>WBI</id>
<version>7.0.0.0</version>
<build-info date="8/31/09" level="of0935.02"/>
</product>
```

Click the following links for appropriate product version and history information:

Table 36. Product version and history information links.

Links
Product version information
genVersionReport command
versionInfo command
historyInfo command
genHistoryReport command

Profile commands in a multiprofile environment

When two or more profiles exist on a server, certain commands require that you specify the profile to which the command applies. These commands use the -profileName attribute to identify which profile to address. To overcome having to specify the -profileName attribute for each command, use the versions of the commands that exist in the bin directory of each profile.

The first profile that you create within one installation of WebSphere Process Server is the default profile. The default profile is the default target for commands issued from the bin directory in the directory where WebSphere Process Server is installed. If only one profile exists on a system, every command operates on that profile. To target a command to a profile other than the default, you must issue the command as follows:

- If you want to issue the command from any directory, follow the command with the -profileName attribute and the fully qualified path to the profile to address. For example:

  startServer -profileName server1

- To overcome having to specify the -profileName attribute for a command, use the version of the command that exists in the bin directory of the profile to address. The directory is one of the following based on platform:

  - `Linux` `UNIX` *profile_root*/bin

  - `Windows` *profile_root*\bin

Special considerations when installing from Passport Advantage

If you plan to install from images obtained from Passport Advantage, you must review the downloading instructions provided with the images and observe certain guidelines concerning user permissions and directory setup.

Images map one-for-one to the *WebSphere Process Server V7.0 DVD* and the *WebSphere Application Server Network Deployment Supplements V7.0* CDs. They are grouped by platform into electronic assemblies. Each assembly contains all the images for that platform, allowing you to quickly identify all software needed for the platform.

Observe the following guidelines when installing from images obtained from Passport Advantage:

- `  Linux    UNIX  ` Ensure that the user who extracts the files with the untar command is the same user who will install the product. The product installer will not work properly if different users perform these tasks.

- Make sure that you extract the contents of the images for *WebSphere Process Server V7.0 DVD* and the *WebSphere Application Server Network Deployment Supplements V7.0* CDs into separate directories. If you extract the files from the images into the same directory, errors will occur. Consider using sibling directories, for example:

  - `  Linux    UNIX  `

    ```
    %/downloads/WPS/image1
    %/downloads/WPS/image2
    ```

  - `  Windows  `

    ```
    C:\downloads\WPS\image1
    C:\downloads\WPS\image2
    ```

Troubleshooting installation and configuration

You can diagnose problems when the installation and configuration of WebSphere Process Server is unsuccessful.

Procedure

1. Read any error messages from the installation process.

   See the following topic for an explanation: Error messages: installation and profile creation and augmentation. If the message corresponds to any of those described, correct the problem, clean up any installed portions, and try to reinstall.

2. If the installation of WebSphere Application Server Network Deployment was not successful, check Troubleshooting installation in the WebSphere Application Server Network Deployment information center and use the information found there to correct the problem before attempting to reinstall WebSphere Process Server.

3. If the installation of WebSphere Application Server Feature Pack for Service Component Architecture (SCA) with the Service Data Objects (SDO) feature not successful, check Troubleshooting installation in the WebSphere Application Server Network Deployment information center and use the information found there to correct the problem before attempting to reinstall WebSphere Process Server.

4. If the installation of WebSphere Feature Pack for Web Services was not successful (and installation of WebSphere Application Server Network Deployment was), check Troubleshooting Web server plug-ins installation and removal in the WebSphere Application Server Network Deployment information center and use the information found there to correct the problem before attempting to reinstall WebSphere Process Server.

   Tip: If a problem occurs during an installation of WebSphere Feature Pack for Web Services as part of a WebSphere Process Server installation, the installation process will not continue and an error message will be displayed.

5. If the installation of WebSphere Process Server was not successful (and installation of WebSphere Application Server Network Deployment and WebSphere Feature Pack for Web Services were), check other WebSphere Process Server installation log files. For information about the names, locations, and descriptions of these log files, see Installation and profile creation log files.

6. If you have successfully created a server profile, use the First steps console or the command-line method to start the server.

7. Verify that the server starts and loads properly by looking for a running Java process and the *Open for e-business* message in the `SystemOut.log` and `SystemErr.log` files.

   If no Java process exists or if the message is not displayed, examine the same logs for any miscellaneous errors. Correct any errors and try again.

   You can find the `SystemOut.log` and `SystemErr.log` files in the following platform-specific directories:

   - Linux UNIX **On Linux and UNIX platforms:** `profile_root`/logs/`servername`

- • Windows **On Windows platforms:** *profile_root*\logs\servername
8. Use the First steps console or the command-line method to stop the server, if it is running.
9. If you want to use a Snoop Servlet to verify the ability of the Web server to retrieve an application from WebSphere Process Server, see the step "Start the Snoop servlet to verify the ability of the Web server to retrieve an application from the Application Server" in Troubleshooting installation in the WebSphere Application Server Network Deployment documentation.
10. Start the administrative console. For more information, see Starting and stopping the administrative console.
11. To resolve any IP address caching problems, see the step "Resolve any IP address caching problems" in Troubleshooting installation in the WebSphere Application Server Network Deployment documentation.

What to do next

On the product support Web site, you can review current information about resolutions to known problems, and you can read documents that can save you time gathering the information that you need to resolve a problem. Before opening a PMR, see the IBM WebSphere Process Server support page.

Messages and known issues during installation and profile creation

Some of the most commonly found error messages encountered when installing and configuring can be addressed with actions that resolve the underlying problems.

Note: Linux UNIX Windows The following WebSphere Process Server installation and configuration errors appear on Linux, UNIX, and Windows platforms.

Tip: For information about messages that might be generated by the installation of WebSphere Application Server Network Deployment, refer to the Business Process Management messages topic.

What kind of problem are you having while installing WebSphere Process Server?
- • "Supported IBM JDK was not found. The IBM JDK shipped with this product must be located at *install_root*/JDK. Correct this problem and try again." on page 144
- • "Warning: Cannot convert string "<type_name>"to type FontStruct" on page 144

If you do not see an error message that resembles yours, or if the information provided does not solve your problem, contact WebSphere Process Server support at IBM for further assistance.

Known issues

Implement the suggested solutions to resolve these known problems related to installation and profile creation.

Table 37. Known issues and solutions for problems related to installation and profile creation

Issue	Problem	Solution
WebSphere Process Server, version 7.0.0.0 and WebSphere Integration Developer, version 7.0.0 cannot coexist in the same package group or WebSphere Process Server, version 7.0.0.0 and Lotus® Forms Designer 3.5.1.0 cannot coexist in the same package group	WebSphere Application Server failed to silently import into Installation manager, so the WebSphere Process Server package cannot find a package group it can install into	WebSphere Application Server installation needs to be properly imported into Installation Manager. Open Installation Manager from the Start Menu, select **Import**, and walk through the Installation Manager wizard to import WebSphere Application Server.
The Launchpad application reports that WebSphere Application Server installed successfully, but there were errors importing into Installation Manager	WebSphere Application Server failed to silently import into Installation Manager. This could have been caused by Installation Manager being open during the silent import call or because of disk issues.	Look in the log for errors: • On Linux: *install_root*/logs/ launchpad_import.txt • On Windows platforms: *install_root*\logs\ launchpad_import.txt If you have run out of disk space, clean up enough space to complete the import, then open Installation Manager from the Start Menu. Then, select **Import** from the Installation Manager wizard and complete the steps to import WebSphere Application Server.
Import log doesn't exist. • On Linux: *install_root*/logs/ launchpad_import.txt • On Windows platforms: *install_root*\logs\ launchpad_import.txt	Installation Manager was open during the silent import call	Open Installation Manager from the Start Menu and select **Import**. Then, complete the steps to import WebSphere Application Server.

Table 37. Known issues and solutions for problems related to installation and profile creation (continued)

Issue	Problem	Solution
The Launchpad application reports that the WebSphere Application Server has failed	Silent install of WebSphere Application Server failed	View the following logs for errors: • On Linux: *install_root*/logs/install/ log.txt • On Windows platforms: *install_root*\logs\install\ log.txt If the logs directory does not exist on your system, the installation failed very early in the process. In this case, review the following log files: • On Linux: *user_home*/waslogs/ log.txt • On Windows platforms: *user_home*\waslogs\ log.txt

Supported IBM JDK was not found. The IBM JDK shipped with this product must be located at *install_root*/JDK. Correct this problem and try again.

If you use symbolic links to point to the IBM Java Development Kit (JDK) shipped with the product, or to a JDK found in the PATH environment variable on your system, IBM SDK for Java validation might fail, resulting in a failed installation. This problem is caused by the way IBM SDK for Java validation code detects whether the JDK shipped with the product is the current JDK used for installation.

To resolve this problem, do not use symbolic links in JVMs supplied with the installation image of WebSphere Process Server and remove symbolic links from all JVMs that appear in your system's PATH environment variable.

Warning: Cannot convert string "<type_name>"to type FontStruct

If you install the Web server plug-ins for WebSphere Application Server, you also install the ikeyman utility. The ikeyman utility is part of the Global Services Kit 7 (GSKit7).

Linux   If you issue the `ikeyman.sh` script on a Linux system, you might see the following message:

```
Warning: Cannot convert string
   "-monotype-arial-regular-r-normal--*-140-*-*-p-*-iso8859-1"
   to type FontStruct
```

You can safely ignore the warning and use the ikeyman utility.

Installation and profile creation log files

Various log files are created during installation and uninstallation of WebSphere Process Server and during profile creation, augmentation, and deletion. Consult the applicable logs if problems occur during these procedures.

Table 38 shows the log file names, locations, and descriptions for success and failure for WebSphere Process Server.

Some directory paths, file names, and indicator values in Table 38 contain spaces to allow the entries to fit in the table cells. The actual directory paths, file names, and indicator values do not contain spaces.

The variable *install_root* represents the installation directory of WebSphere Process Server. The variable *profile_root* represents the root location of a profile.

For more information see "Default installation directories for the product and profiles" on page 127.

Table 38. Installation and profile logs for WebSphere Process Server components

Log name and location	Log description
• `Linux` `UNIX` *install_root*`/logs/install/log.txt` • `Windows` *install_root*`\logs\install\log.txt` If the logs directory does not exist on your system, the installation failed very early in the process. In this case, review the following log files: • `Linux` `UNIX` *user_home*`/waslogs/log.txt` • `Windows` *user_home*`\waslogs\log.txt`	WebSphere Application Server installation log files
• `Linux` `UNIX` *install_root*`/logs/launchpad_import.txt` • `Windows` *install_root*`\logs\launchpad_import.txt`	All errors and warnings related to the import of WebSphere Application Server from the launchpad application
• `Linux` `UNIX` *install_root*`/logs/wbi/install/installconfig_server.log` • `Windows` *install_root*`\logs\wbi\install\installconfig_server.log`	Logs configuration actions that run at the end of the installation process to configure components, install system applications, and create Windows shortcuts and registry entries.
• `Linux` `UNIX` *install_root*`/logs/manageprofiles/pmt.log` • `Windows` *install_root*`\logs\manageprofiles\pmt.log`	Logs all events from the Profile Management Tool.
• `Linux` `UNIX` *install_root*`/logs/manageprofiles/profile_name_create.log` • `Windows` *install_root*`\logs\manageprofiles\profile_name_create.log`	• Traces all events that occur during the creation of the named profile. • Created when a profile is created during a Complete installation, when using the Profile Management Tool, or when using the manageprofiles command-line utility.

Table 38. Installation and profile logs for WebSphere Process Server components (continued)

Log name and location	Log description
• ` Linux ` ` UNIX ` *install_root*/logs/manageprofiles/ *profile_name*_create_error.log • ` Windows ` *install_root*\logs\wbi\update\ *profile_name*_create_error.log	Logs information extracted from the*profile_name*_create.log file. This information pertains to any failing configuration actions, validations, wsadmin calls and or any corresponding log files.
• ` Linux ` ` UNIX ` *install_root*/logs/manageprofiles/ *profile_name*_augment.log • ` Windows ` *install_root*\logs\manageprofiles\ *profile_name*_augment.log	• Traces all events that occur during the augmentation of the named profile. • Created when a profile is augmented, when using the Profile Management Tool, or when using the manageprofiles command-line utility.
• ` Linux ` ` UNIX ` *install_root*/logs/manageprofiles/ *profile_name*_augment_error.log • ` Windows ` *install_root*\logs\wbi\update\ *profile_name*_augment_error.log	Logs information extracted from the *profile_name*_augment.log file. This information pertains to any failing configuration actions, validations, wsadmin calls and any corresponding log files.
• ` Linux ` ` UNIX ` *install_root*/logs/manageprofiles/ *profile_name*_delete.log • ` Windows ` *install_root*/logs/manageprofiles/ *profile_name*_delete.log	• Traces all events that occur during the deletion of the named profile. • Created when profile deletion is performed with the manageprofiles command-line utility.
• ` Linux ` ` UNIX ` *install_root*/logs/wbi/uninstall/ uninstallconfig_server.log • ` Windows ` *install_root*\logs\wbi\uninstall\ uninstallconfig_server.log	Logs all uninstallation events relating to WebSphere Process Server.
• ` Windows ` *Agent data location*\logs Typically: C:\Documents and Settings\All Users\Application Data\IBM\Installation Manager\logs • ` Linux ` ` UNIX ` *Agent data location*/logs Typically: /var/ibm/InstallationManager/logs	Installation Manager log file directory under the *Agent data location*. For more information on the *Agent data location* refer to the Installation Manager documentation.
• ` Windows ` *install_root*\logs*product shortname*\ silent_install.log • ` HP-UX ` ` Linux ` ` Solaris ` *install_root*/logs/ *product shortname*/silent_install.log • ` AIX ` *install_root*/logs/*product shortname*/ silent_install.log	Log files containing the high-level error messages related to a silent installation ◄ for silent install log you have: install_root\logs\silent_install.log install_root/logs/silent_install.log install_root/logs/silent_install.log it should actually be install_root\logs\<product shortname>/ silent_install.log install_root/logs/<product shortname>/silent_install.log install_root/logs/ <product shortname>/silent_install.log

Troubleshooting the launchpad application or First Steps

If the launchpad application or First Steps does not start, try the following troubleshooting tips.

Troubleshooting the launchpad application

Restart the launchpad after you make any changes.

- If you are using images from Passport Advantage, make sure that you extract the contents of the images for *WebSphere Process Server Version 7.0* DVD, *WebSphere Application Server Network Deployment Supplement Version 7.0* CDs, and *WebSphere Portal add-in for WebSphere Process Server* DVD into separate directories. Extracting the files from the images into the same directory will cause errors to occur. It is recommended that you use sibling directories. For example, use a set of directories such as the following:

  – `Linux`　`UNIX`

    ```
    %/downloads/WPS/image1
    %/downloads/WPS/image2
    %/downloads/WPS/image3
    ```

  – `Windows`

    ```
    C:\downloads\WPS\image1
    C:\downloads\WPS\image2
    C:\downloads\WPS\image3
    ```

- If you can start the launchpad, but selecting a link does not resolve to a page in the launchpad, you might have the media for the wrong operating system in the disk drive. Check the validity of the media.

- `Windows` If you are attempting to use the Mozilla browser on a Windows system, Internet Explorer might open instead. The launchpad does not recognize Mozilla as the default browser if Internet Explorer is also installed on the same system. The launchpad is fully functional with Internet Explorer, so no action is required.

  To create an environment variable that forces the use of Mozilla, issue the following case-specific command at a command prompt:

  `set BROWSER=Mozilla`

- Ensure that the JavaScript™ function is enabled in your browser.

  `Linux`　`UNIX` Mozilla: Click **Edit > Preferences > Advanced > Scripts & Plugins**:

  – Enable JavaScript for: Navigator.
  – Allow scripts to ... (Select all boxes.)

  `Linux`　`UNIX` Mozilla Firefox: Click **Tools > Options > Content**:

  – Select **Enable Java**.
  – Select **Enable JavaScript**.
  – Click **Advanced** and Allow scripts to ... (Select all boxes.)

  `Windows` Internet Explorer: Click **Tools > Internet Options > Security > Custom Level for Internet > Scripting > Active scripting > Enable**.

If the launchpad links still do not work after trying these tips, start the component installation programs directly.

Troubleshooting First Steps

If links from the First Steps console fail to open browser windows, or the First Steps console fails to launch, or immediately quits, on the Microsoft Windows operating system when Mozilla Firefox is set as the default browser, try the following workarounds.

- Modify the Windows registry to delete the spaces in the location name:
  1. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Clients\StartMenuInternet\ FIREFOX.EXE\shell\open\command`

Note: The preceding line might be word-wrapped. Be sure to navigate to the location specified in the preceding lines, up to the "`command`" key in the registry.

2. Change the "(Default)" entry so that spaces are removed from the path.

   For example, if the path is set as "`C:\Program Files\Mozilla Firefox\firefox.exe`", change the path to its short equivalent "`C:\Progra~1\Mozill~1\firefox.exe`".

   The short names might not be the same on all systems. For example, if you have installed "Mozilla Thunderbird" as well as "Mozilla Firefox," and both are installed in the "Program Files" directory, the short name to the location of Mozilla Firefox might be different than the example above. You can use the "`dir /X`" command to determine the short names of individual files and directories located in the current directory.

   Note: If you choose this option, be careful that you do not corrupt the Windows registry. This key might vary for different locales, so use caution or choose another workaround. It is recommended that you backup the registry before making nay changes.

- Install Mozilla Firefox to a different location which does not contain spaces.
- Change the default browser temporarily.
   1. Set Windows Internet Explorer as the default browser.
   2. Reset Mozilla Firefox as the default browser. This automatically changes the registry entry in the first workaround so that the spaces are removed.

      This only works when you set the default browser from within the Mozilla Firefox application. It will not work when using the "*Set Program Access and Defaults*" command in "*Add/Remove Programs*".

Troubleshooting a silent installation

If a silent installation using a response file fails, you can examine log files and error messages to determine what went wrong, and make changes to your response file.

Before you begin

For information about using the response file for a silent installation of WebSphere Process Server, see "Silently installing WebSphere Process Server" on page 53.

To troubleshoot a silent product installation, perform the following steps.

Procedure

1. Check the `run_templates` script to ensure that you are specifying the correct parameters. This script is located in the *install_image*/`wbi` directory.
2. Check your response file to make sure you have specified the correct option values to ensure that the Installation Manager program can read the values. Incorrect specifications affect the silent interface of the installation wizard. For example, always use the correct case within property names, which are case-sensitive. In addition, always enclose values in double quotation marks. If the error is an incorrect option value, the Installation Manager program displays a warning message that you must confirm and stops the installation.
3. Compare your response file to the `template_response.xml` file template that is shipped with the product to make the necessary corrections. This file is located in the *install_image*/`wbi` directory. After correcting the file, reinstall.

4. Review commonly found error messages in Messages: installation and profile creation and augmentation.

5. Examine log files. See the descriptions of relevant log files listed in Installation and profile creation log files.

6. For other tips on troubleshooting your installation, see Troubleshooting installation.

7. If your profile did not create successfully, see Recovering from profile creation or augmentation failure.

Diagnosing a failing Ant configuration script

Determine whether a product installation problem on an operating system is caused by a failing Apache Ant configuration script.

Before you begin

Start diagnosing installation problems by looking at the troubleshooting procedure. See Troubleshooting installation and configuration. After the installation completes successfully, several Ant scripts configure the product. The following procedure describes what to do when an Ant script fails. When the installation log does not indicate a failure, determine how to correct any problems with failing Ant configuration scripts.

About this task

The *install_root*/logs/wbi/install/installconfig_server.log file, when present, describes any failure of an Ant script. Determine if any of the following configuration scripts failed. If so, use the configuration script recovery procedures. Use the investigative action to manually verify that the following configuration scripts ran successfully during the configuration of the WebSphere Process Server product. If any script failed, use the recovery action steps to complete the function of the script.

To diagnose failed Ant configuration scripts, perform the following steps.

Procedure

- Diagnose the failed `90SConfigWBIMigrationScript.ant` configuration script. This script changes the permissions of the following script to 755: *install_root*/bin/BPMMigrate. This script also replaces the following tokens in the *install_root*/bin/BPMMigrate script:

From:	To the value that you selected during installation:
`${JAVAROOT}`	*install_root*/java/jre/bin/java
`${MIGRATIONJAR}`	*install_root*/bin/migration/migrationGUI/migrationGUI.jar
`${WASROOT}`	*install_root*
`${PRODUCTID}`	`${WS_CMT_PRODUCT_TYPE}`

  1. Investigative action: Verify that the permissions are 755 for the following directories:

     – Linux   UNIX   *install_root*/bin/BPMMigrate.sh

     – Windows   *install_root*\bin\BPMMigrate.bat

2. Recovery action: Issue the following command:

   – `Linux` `UNIX` `chmod 755 `*`install_root`*`/bin/BPMMigrate.sh`

   – `Windows` `chmod 755 `*`install_root`*`\bin\BPMMigrate.bat`

3. Investigative action: Open the following file in an editor and verify that real values exist instead of the following values: `${JAVAROOT}`, `${MIGRATIONJAR}`, `${WASROOT}`, and `${PRODUCTID}`.

   – `Linux` `UNIX` *`install_root`*`/bin/BPMMigrate.sh`

   – `Windows` *`install_root`*`\bin\BPMMigrate.bat`

4. Recovery action: Change the following tokens to values in the `BPMMigrate` script: `${JAVAROOT}`, `${MIGRATIONJAR}`, `${WASROOT}`, and `${PRODUCTID}`.

- Diagnose the failed `85SConfigNoProfileFirstStepsWBI.ant`. This script copies all files from the *`install_root`*`/properties/version/install.wbi/firststeps.wbi` directory to the *`install_root`*`/firststeps/wbi/html/noprofile` directory. This script also replaces the following tokens in the following files:

   – `Linux` `UNIX` *`install_root`*`/firststeps/wbi/firststeps.sh`

   – `Windows` *`install_root`*`\firststeps\wbi\firststeps.bat`

From:	To the value that you selected during installation:
`${JAVAROOT}`	*`install_root`*`/java/jre/bin/java`
`${PROFILEROOT}`	*`install_root`*
`${HTMLSHELLJAR}`	*`install_root`*`/lib/htmlshellwbi.jar`
`${CELLNAME}`	`${WS_CMT_CELL_NAME}`

1. Investigative action: Verify that all files are copied from the *`install_root`*`/properties/version/install.wbi/firststeps.wbi` directory to the *`install_root`*`/firststeps/wbi/html/noprofile` directory.

2. Recovery action: Copy all of the files from the *`install_root`*`/properties/version/install.wbi/firststeps.wbi` directory to the *`install_root`*`/firststeps/wbi/html/noprofile` directory.

3. Investigative action: Open the *`install_root`*`/firststeps/wbi/firststeps` script in an editor. Verify that real values exist instead of the following values: `${JAVAROOT}`, `${PROFILEROOT}`, `${HTMLSHELLJAR}`, and `${CELLNAME}`.

4. Recovery action: Change the following tokens to values in the *`install_root`*`/firststeps/wbi/firststeps` script. `${JAVAROOT}`, `${PROFILEROOT}`, `${HTMLSHELLJAR}`, and `${CELLNAME}`.

Results

After you correct any installation errors and any Ant script configuration errors by performing the corrective actions in this procedure, the installation is complete.

What to do next

Start the First steps console.

Recovering from profile creation or augmentation failure

The Profile Management Tool can experience failures when creating new or augmenting existing profiles. The same can occur using the manageprofiles command-line utility. If such a failure occurs, first check the log files as described in this topic, then follow the recovery instructions described, depending on the situation.

Log files

All manageprofiles log files are in *install_root*/logs/manageprofiles. Look at the following log files in the order given. Each log file must contain the entry "INSTCONFSUCCESS." If a file does not include this entry, a failure was detected. Look at the log files to determine why a failure was encountered and to determine a remedy.

1. The log file *profile_name*_create_error.log (where *profile_name* is the name of the profile).

   Note: Look at this file only if you were creating a new profile, not augmenting an existing one.

   - `Linux` `UNIX` *install_root*/logs/manageprofiles/ *profile_name*_create_error.log

   - `Windows` *install_root*\logs\wbi\update*profile_name*_create_error.log

   Search for the text `Configuration action succeeded` or `Configuration action failed`.

   Note: There can be multiple occurrences of `Configuration action failed`. Investigate and remedy each one. Also review the log files described in the following options, if the profile was created.

   Note: Additional information is available in the `manageprofiles` directory in the pmt.log, which logs all events that occur when a default profile is created during a complete installation using the Profile Management Tool.

2. Log file *profile_name*_augment_error.log (where *profile_name* is the name of the profile).

   This log file is located in the following directories:

   - `Linux` `UNIX` *install_root*/logs/manageprofiles/ *profile_name*_augment_error.log

   - `Windows` *install_root*\logs\wbi\update*profile_name*_augment_error.log

   Search for the text `Configuration action succeeded` or `Configuration action failed`.

   Note: There can be multiple occurrences of `Configuration action failed`. Investigate and remedy each one. Also review the log files described in the following options, if the profile was created.

   Note: If you want to know the status of a profile you created during installation, run the following commands:

   - `Linux` `UNIX` *install_root*/bin/logProfileErrors.sh

   - `Windows` *install_root*\bin\logProfileErrors.bat

3. Individual profile template action log files.

If you discovered false values in the log files described in the preceding options, review the log files in the following directories:

- `Linux` `UNIX` `install_root`/logs/manageprofiles/`profile_name` on Linux and UNIX systems
- `Windows` `install_root`\logs\manageprofiles\`profile_name` on Windows systems

where *profile_root* or *user_data_root* is the installation location of the profile.

These log files do not follow a consistent naming convention, but typically, each is the name of the Apache Ant script that failed followed by `.log`. For example, suppose the following entry is in the `profile_name_augment.log` file:

```
<messages>Result of executing
E:\o0536.15\profileTemplates\default.wbicore\actions\saveParamsWbiCore.ant
was:false</messages>
```

First look at the surrounding entries in the `profile_name_augment.log` file in the `install_root`/logs/manageprofiles directory. If you cannot determine the cause of the failure from the surrounding entries, look for the corresponding log file for any failing Ant script entries. In this case, the log file created by the `saveParamsWbiCore.ant` script is `saveParamsWbiCore.ant.log`. Look at that file to investigate why the failure occurred.

Recovery for creation failure

After you determine why profile creation failed and address the cause of the failure, you can try to create the profile again.

Note: When you create a profile, it first creates a WebSphere Application Server profile and then augments it with WebSphere Process Server profile templates to create a WebSphere Process Server profile. Even if you encountered a profile creation failure, a profile can exist that does not have all the needed augmentations.

To determine if the profile exists, run the `install_root`/bin/manageprofiles `-listProfiles` command. If the profile name you used for creation does not exist, you can re-create the profile. If the profile name you used for creation exists, then the profile was created and you have encountered an augmentation failure. For tips on recovering from an augmentation failure, see "Recovery for augmentation failure."

Recovery for augmentation failure

After you determine why profile augmentation failed and address the cause of the failure, you can try to augment the existing profile again to successfully create a complete WebSphere Process Server profile by following these steps:

1. Start the Profile Management Tool and, instead of creating a new profile, choose to augment an existing profile.
2. Choose the profile you were working with, and enter the correct information for it.

Note: Some of the augmentations might have completed successfully the first time you ran the Profile Management Tool. As a result, you might not see all of the panels that you saw the first time you tried to create the profile. This is because the Profile Management Tool detects which remaining augmentations must be completed and displays only the necessary panels.

Troubleshooting the Business Process Choreographer configuration

For information on how to solve problems relating to the configuration of Business Process Choreographer, go to the WebSphere Process Server for Multiplatforms, version 7.0, information center and review the topics under **Installing WebSphere Process Server > Troubleshooting installation and configuration > Troubleshooting the Business Process Choreographer configuration**. You can also find this information in the *Business Process Choreographer PDF*.

Configuring WebSphere Process Server

After you have installed WebSphere Process Server, you must complete additional configuration tasks to fully prepare your runtime environment.

Common configurations

There are several common configurations that you can create using WebSphere Process Server.

You can create a stand-alone configuration or network deployment configuration that can support several different *patterns*.

Stand-alone and Network Deployment configuration differences

You can choose to configure WebSphere Process Server using a stand-alone configuration or a network deployment configuration.

For a stand-alone configuration, you can configure all of the components during the profile creation by using either the Profile Management Tool or manageprofiles command-line utility.

Using the Profile Management Tool to create a stand-alone configuration, results in a single JVM on a single node that is implicitly created.

For a network deployment environment, you create a deployment manager profile and then configure the components on a single cluster or several clusters (as opposed to a single server).

You can configure the components in a network deployment configuration using the administrative console through dedicated console pages or you can use the deployment environment wizard. Additionally, you can configure the components of your network deployment environment using scripts with individual administrative commands.

The following table contains specifics on the differences between a standalone configuration and Network Deployment configuration.

Table 39. Standalone and Network Deployment configuration differences.

The following table describes 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 . Set up additional servers within the node through the administrative console or scripting.	Set up each deployment manager node through the Profile Management Tool . Add application server nodes to the Network Deployment cell through the Profile Management Tool .

Table 39. Standalone and Network Deployment configuration differences (continued).

The following table describes the differences between a WebSphere Application Server for z/OS standalone cell and Network Deployment cell.

	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 and are managed by a deployment manager server.
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.
Clustering available?	No	Yes

Related tasks

Creating profiles
You can create new WebSphere Enterprise Service Bus or WebSphere Process Server profiles interactively by using the Profile Management Tool graphical user interface (GUI) or from a command line by using the manageprofiles command-line utility.

Creating deployment environments
Setting up deployment environments involves creating the deployment environment definition and then generating the environment.

Creating a Network Deployment configuration

Creating a network deployment configuration involves installing WebSphere Process Server, creating the appropriate profiles and configuring the deployment environment.

The steps leading up to configuring the deployment environment are replete with options specific to the type of configuration you are creating and the manner by which you create it. WebSphere Process Server provides flexibility in how to create a network deployment configuration.

The decisions that you make at profile creation time can effect the task flow (the sequence of steps and the path through the configuration process) for creating a network deployment configuration.

This topic provides a roadmap for creating a network deployment configuration. It does not represent the only way to create the network deployment configuration, but it does represent a way that has been tested and validated. The process described in this topic assumes a topology based on the supplied pattern type of *remote messaging and remote support*.

Remote messaging and remote support is a standard topology for network deployment configuration. This topology is also referred to as the gold topology in some publications. Remote messaging and remote support is the preferred topology for WebSphere Process Server production environments because it is both scalable (you can expand the topology to meet changing business demands) and because the each of the distinct functions within WebSphere Process Server is divided among the three clusters, you can pinpoint performance bottlenecks and adjust the cluster size fairly easily.

The following diagram illustrates the logical components of a remote messaging and remote support topology pattern for a Network Deployment configuration. The terms that display are defined following the diagram.
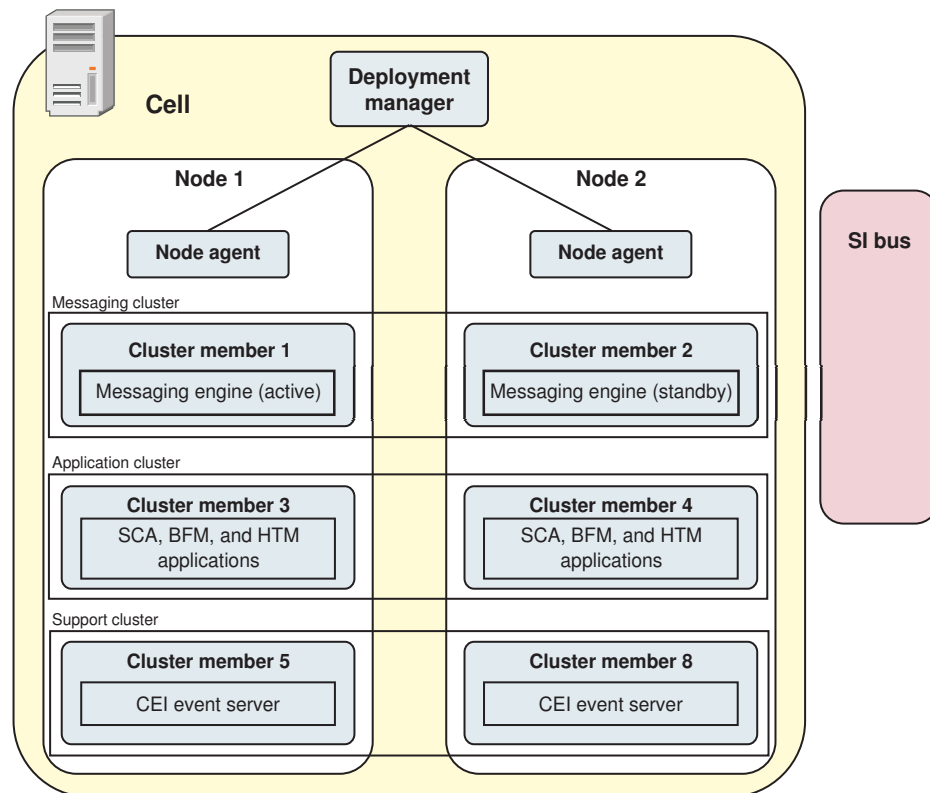
The terms in the diagram are defined below.

Cell   Cells are logical groupings of one or more nodes in a WebSphere Process Server distributed network.

    A cell is a configuration concept, a way for administrators to logically associate nodes with one another. Administrators define the nodes that make up a cell, according to the specific criteria that make sense in their organizational environments.

Deployment Manager

    A deployment manager is a server that manages operations for a logical group, or cell, of other servers. The deployment manager is the central location for administering the servers and clusters.

    Administrators use the administrative console of the deployment manager to manage the servers and clusters in the cell. Activities performed from the Deployment manager include the following:

- configuring servers and clusters
- adding servers to clusters
- starting and stopping servers and clusters
- deploying Service Component Architecture (SCA) modules to servers and clusters

    You can create the deployment manager after installation using several different methods.

Node A node is a logical grouping of managed servers. A node usually corresponds to a logical or physical computer system with a distinct IP host address.

Nodes cannot span multiple computers. Node names usually are identical to the host name for the computer. Nodes in the network deployment topology can be managed or unmanaged. A managed node has a node agent process that manages its configuration and servers. Unmanaged nodes do not have a node agent.

Node Agent

Node agents are administrative agents that route administrative requests to servers.

A node agent is a server that runs on every host computer system that participates in the Network Deployment configuration

Clusters

Clusters are groups of servers that are managed together and participate in workload management.

A cluster can contain nodes or individual application servers.

You can create clusters for specific purposes. The topology diagram above shows 3 clusters, each with its own functions and applications. The remote messaging and remote support topology pattern includes at least 3 clusters.

• All of the applications are deployed to the Application Cluster.

Business Process Choreographer is configured in the Application Cluster, so each cluster member has a business process container and a human task container.

• The Messaging Cluster is a member of all four of the required WebSphere Process Server buses (SI Bus):

– SCA.SYSTEM

– SCA.APPLICATION

– CEI

– BPC

• The Support Cluster is the cluster on which you configure all of the supporting infrastructure applications, such as:

– Business Process Choreographer tools (Business Process Choreographer Explorer and the Explorer reporting function)

– Business Rules Manager

– Common Event Infrastructure (CEI)

– Business Space

Cluster members

An identically configured copy of an object, such as an application server. Cluster members can be used for workload management purposes, for example, to support horizontal scaling and vertical scaling.

The information in this topic assumes not only a particular path through the process for creating a network deployment environment, but also assumes that you select specific options presented to you by the Profile Management Tool (PMT) and the Deployment Environment Configuration wizard.

The sections that follow present a specific path through the configuration process for creating a network deployment environment. The information presented in

each section states explicitly which path to take and what options to choose, but also contains references to existing topics in the information center that provide explanations on the all available choices and options. The links to existing topics in the information center reside in the related information section of this topic.

Related concepts

"Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 This topic discusses reserved terms and issues you must consider when naming your profile, node, server, host and cell (if applicable).

Installing WebSphere Process Server - Assumptions for Network Deployment configuration

For the Network Deployment configuration task flow presented in this topic, we make certain assumptions regarding the type of installation.

Before you begin

The network deployment configuration is based on the remote messaging and remote support pattern. View the description of the remote messaging and remote support topology in the planning section of the information center.

Be aware that remote messaging and remote support topology is sometimes referred to as the "gold topology" in various information resources outside of the WebSphere Process Server information center.

About this task

The WebSphere Process Server installation procedure is fully documented in the section on Installing the software.

It is assumed that you have read about the different ways to install the software and that you have chosen the method best suits your needs and skill set.

it is assumed that you have not created the common database manually before installing the product, but that you will create the common database at profile creation time.

Procedure

1. Determine how you want to place the installation files on your system as documented in the *Installation overview*.
2. Place the files or installation image on your system, using the method of your choice, as described in the scenarios in *Installation overview*
3. Use Installation Manager to complete the installation

What to do next

After you have installed WebSphere Process Server you need to plan out your profile creation process and then create the profiles that are appropriate for a Network Deployment configuration.

Deciding how to create profiles and how to create the common database for a Network Deployment configuration

WebSphere Process Server supports several different methods for creating profiles and creating the common database that WebSphere Process Server uses.

The supported methods for creating the deployment manager profile configuration include the following:

- Using the Profile Management Tool to:
  - Create advanced deployment manager profiles
  - Create typical deployment manager profiles
  - Create Deployment environment deployment manager profiles
- Using the managed profile commands to create a deployment manager profile.

The supported methods for creating the common database in a network deployment configuration include the following:

- Creating the common database before product installation

  If your organization requires that the database be created by a user with DBA privileges, that user must create the common database before creating or augmenting profiles.

  The scripts must be customized by you or the database administrator before you can use them to create and configure the database

- Creating the database design file using the database design tool (DDT).

  The DDT generates the design file from a user specified properties file or user interactive input. The resulting design file is then used by the DDT to create the database scripts. You can import the database design at profile creation time to simplify the database configuration portion of the profile creation process. For more information see, *Creating the database design file using the database design tool* in the **Configuring** section of the information center.

- Creating the common database immediately after product installation.

  The WebSphere Process Server creates a directory that holds scripts for creating the common database. After installingWebSphere Process Server you can navigate to the directory and run the scripts manually.

  The scripts must be customized by you or the database administrator before you can use them to create and configure the database

- Creating the common database and the database tables as part of profile creation.

  When you use the Profile Management Tool (PMT) to create the deployment manager profile, the tool can create the common database and run the scripts to create the database tables automatically.

- Creating the common database as part of profile creation, but delay running the scripts to create the database tables.

  When you use the Profile Management Tool (PMT) to create the deployment manager profile, you can set parameters so that the tool creates the common database but does not run the database scripts to create the database tables automatically.

  If you choose to delay the execution of the database scripts, then the PMT tool does not run the scripts to create the database tables, instead it only generates the scripts, which you or the database administrator must run manually in order to create the required database tables.

The following section presents information on creating an advanced deployment manager profile using the Profile Management Tool, with a decision to delay the execution of the database scripts until after profile creation.

Creating advanced deployment manager profile using the Profile Management Tool

Learn how to use the Advanced option of the Profile Management Tool to create and configure WebSphere Process Server deployment manager profiles. Selecting the Advanced option creates profiles with customized configuration settings.

Before you begin

The software is installed on your system.

Restrictions:

- You cannot use the Profile Management Tool to create or augment profiles on WebSphere Process Server installations on 64-bit architectures except on the Linux on zSeries® platform. To create profiles on other 64-bit architectures, you can use the manageprofiles command-line utility. For information about using the manageprofiles command-line utility, see "Creating profiles using the manageprofiles command-line utility" on page 253. You can also use the Profile Management Tool on these architectures if you use a WebSphere Process Server 32-bit installation.

- `Vista` `Windows 7` **Restriction for nonadministrative users with multiple instances:** If you install multiple instances of WebSphere Process Server as the root user and give a nonadministrative user access to only a subset of those instances, the Profile Management Tool does not function correctly for the nonadministrative user. In addition, a `com.ibm.wsspi.profile.WSProfileException` or `Access is denied` message occurs in the *install_root*`\bin\ProfileManagement\pmt.bat` file. By default, nonadministrative users do not have access to the `Program Files` directory, which is the default installation location for the product. To resolve this issue, nonadministrative users can install the product or be given permission to access the other product instances.

`Linux` `UNIX` `Windows` The language of the Profile Management Tool is determined by the default language on the system. If the default language is not one of the supported languages, then English is used. You can override the default language by starting the Profile Management Tool from the command line and using the `java user.language` setting to replace the default language. Run the following command:

- `Linux` `UNIX` *install_root*`/java/bin/java -Duser.language=`*locale* *install_root*`/bin/ProfileManagement/startup.jar`

- `Windows` *install_root*`\java\bin\java -Duser.language=`*locale* *install_root*`\bin\ProfileManagement\startup.jar`

For example, to start the Profile Management Tool in the German language on a Linux system, type the following command:

```
install_root/java/bin/java -Duser.language=de install_root/ \
bin/ProfileManagement/startup.jar
```

About this task

This task describes how to create an advanced deployment environment profile using the profile management tool.

Procedure

1. Start the WebSphere Process Server Profile Management Tool.

   Use one of the following commands:

   - Linux   UNIX *install_root*/bin/ProfileManagement/pmt.sh

   - Windows *install_root*\bin\ProfileManagement\pmt.bat

   See the topic "Starting the Profile Management Tool" on page 199 for other methods of starting this tool.

   The Welcome page is displayed.

2. In the Welcome page, click the **Launch Profile Management Tool** button or the **Profile Management Tool** tab.

   The **Profiles** tab is displayed.

3. In the **Profiles** tab, click **Create**.

   The **Profiles** tab can contain a list of profiles that have been created on your machine. For this procedure, it is assumed you are creating a new profile, not augmenting an existing one. If you want to augment an existing version 7.0 profile, see the topic "Augmenting profiles using the Profile Management Tool" on page 301.

   The Environment Selection page opens in a separate window.

4. In the Environment Selection page, expand WebSphere Enterprise Service Bus or WebSphere Process Server and select the type of profile you want to create. Then click **Next**.

   You can also create WebSphere Application Server profiles with this Profile Management Tool. However, this documentation addresses creating WebSphere Enterprise Service Bus or WebSphere Process Server profiles only.

   The Profile Creation Options page is displayed.

5. In the Profile Creation Options page, choose to perform a an **Advanced** profile creation, and click **Next** to display the Optional Application Deployment page.

   The **Advanced** option lets you specify your own configuration values for a profile.

   By selecting the **Advanced** option, you can do the following:
   - Assign customized values to ports, to the location of the profile, and to the names of the profile, node, host, and cell (when applicable).
   - Configure the Common database.
   - Deploy the administrative console.
   - Enable administrative security.
   - Create a system service to run the server, if your operating system and the privileges of your user account permit the creation of services.
   - Optionally: Configure the database using a database design file.

6. In the Optional Application Deployment page, select whether to deploy the administrative console to the profile environment you are creating, then click **Next**.

   The administrative console is a Web-based tool that manages the server. To choose to deploy the administrative console, leave the **Deploy the administrative console (recommended)** check box selected. Clear the check box to deselect it.

   The Profile Name and Location page is displayed.

7. In the Profile Name and Location page, perform the following steps.

   a. Specify a unique name and directory path for the profile, or accept the defaults.

Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name. If you choose not to use the default name, see "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about issues you must consider when naming the profile, such as restrictions on the length of the directory name.

The directory you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. By default, this directory location is:

- `Linux` `UNIX` *install_root*/profiles/*profile_name*

- `Windows` *install_root*\profiles*profile_name*

where *profile_name* is the name you specified. An error message is displayed if:

- The *profile_name* you specify is not unique.
- The directory you specify is not empty.
- Your user ID does not have sufficient permissions for the directory.
- There is insufficient space to create the profile.

b. You can make the profile that you are creating the default profile (so that commands work automatically with it) by selecting the **Make this profile the default** check box. This check box appears only if you have an existing profile on your system.

The first profile that you create on a workstation is the default profile.

The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies. See "Profile commands in a multiprofile environment" on page 139 for more information.

c. Click **Next**. (If you click **Back** and change the name of the profile, you might have to manually change the name on this page when it is displayed again.)

The Node, Host, and Cell Names page is displayed.

8. In the Node, Host, and Cell Names page, specify the node, host, and cell names for the deployment manager, or accept the defaults and click **Next**. Try to keep the node name as short as possible, but ensure that node names are unique within your deployment environment. See "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and other issues you must consider when naming.

The Administrative Security page is displayed.

9. Optionally enable administrative security.

You can enable administrative security now, or later from the administrative console. To enable administrative security now, leave the **Enable administrative security** check box selected, supply a user name and password to log on to the administrative console, and click **Next**. To disable administrative security, clear the check box. To enable administrative security later from the administrative console, open the console and select **Security > Business Integration Security**.

The Security Certificate (Part 1) page is displayed.

10. In the Security Certificate (Part 1) page, create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

    You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

    When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

    The Security Certificate (Part 2) page is displayed.

11. In the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next**.

    If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

    When you create either or both certificates, or import either or both certificates, the keystore files that are created are:

    - `key.p12`: Contains the default personal certificate.
    - `trust.p12`: Contains the signer certificate from the default root certificate.
    - `root-key.p12`: Contains the root signing certificate.
    - `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower® signer certificate are in this keystore file.
    - `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
    - `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

    These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify.

    An imported certificate is added to the `key.p12` file or the `root-key.p12` file.

    If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

12. Verify that the ports specified for the profile are unique and click **Next**.

    The Profile Management Tool detects ports currently used by other WebSphere products and displays recommended port values that do not conflict with existing ones. If you have applications other than WebSphere ones that use specified ports, verify that the ports do not conflict. If you chose not to deploy the administrative console from the Optional Application Deployment page, the administrative console ports are not available on the Port Values Assignment page.

Ports are recognized as being in use if the following conditions are satisfied:
- They are assigned to a profile created under an installation performed by the current user.
- They are currently in use.

Although the tool validates ports when you access the Port Values Assignment page, port conflicts can still occur resulting from selections you make on subsequent Profile Management Tool pages. Ports are not assigned until profile creation completes.

If you suspect a port conflict, you can investigate it after the profile is created. Determine the ports used during profile creation by examining the following file:

- `Linux`   `UNIX`   *profile_root*/properties/portdef.props

- `Windows`   *profile_root*\properties\portdef.props

Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in an existing profile in the WebSphere Application Server Network Deployment information center. Run the `updatePorts.ant` file through the ws_ant script detailed in this topic.

The next step depends on your platform and whether you are installing as a root (Administrator) or nonroot user.

Installation type	Next step
On a Linux or Windows platform, *with root or Administrator group privileges*	The Linux or Windows Service Definition page is displayed. Proceed to step 13.
On any other platform, or as a nonroot user on a Linux or Windows platform	The Database Configuration page is displayed. Proceed to step 15 on page 166.

13. `Linux`   `Windows`   Choose whether to run the process as a Windows service on a Windows platform or as a Linux service on a Linux platform and click **Next**.

    `Windows`   The Windows Service Definition page is displayed for the Windows platform only if the ID that installs the Windows service has the Administrator group privilege. If the profile is configured as a Windows service, the product starts Windows services for processes started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Windows service and issue the startServer or startManager commands, the wasservice command starts the defined services.

    Important: If you choose to log on as a specified user account, you must specify the user ID and the password for the user who is to run the service, and the startup type (default is `Manual`). The user ID must not have spaces in its name, it must belong to the Administrator group, and it must have the advanced user right "Log on as a service." If the user ID belongs to the Administrator group, the Profile Management Tool grants it the advanced user right if it does not already have it.

    During profile deletion, you can remove the Windows service that is added during profile creation.

    IPv6 considerations when running profiles as Windows services

    Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as Local System. Create a user-specific environment variable to enable IPv6. Because this environment variable is a user variable instead of a Local System variable, only a Windows service that

runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as Local System. When the WebSphere Process Server or WebSphere Enterprise Bus Windows service tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the WebSphere Process Server or WebSphere Enterprise Bus Windows service runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as Local System.

Linux The Linux Service Definition page is displayed only if the current operating system is a supported version of Linux and the current user has the appropriate permissions.

WebSphere Process Server attempts to start Linux services for processes that are started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Linux service and issue the startServer or startManager commands, the wasservice command starts the defined services.

By default, WebSphere Process Server is not selected to run as a Linux service.

To create the service, the user who runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, the Linux Service Definition page is not displayed, and no service is created.

You must specify a user name under which the service runs.

To delete a Linux service, the user must be the root user or have proper privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service on behalf of the user.

14. Optional: Configure the databases using a design file. This option is available for both Advanced stand-alone server and Advanced deployment manager profiles.

    a. Select **Use a database design file for database configuration**.
    b. Click **Browse**.
    c. Specify the fully qualified path name for the design file.
    d. Click **Next**.

    If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating the database design file using the database design tool" on page 431.

15. In the Database Configuration page, configure the Common database used by the selected product components.

    If you do not import the database design file, you must configure the database using the database configuration panels.

    Selected WebSphere Process Server components require a database, called the *Common* database, and a Common Event Infrastructure local database to operate. Using values you provide on the Database Configuration pages, the Profile Management Tool automatically creates the Common database and, for stand-alone server profiles, the Common Event Infrastructure database on a local system. It also creates all required tables. You must configure these databases to have a working installation.

    The following WebSphere Process Server components use the Common database:

- Application Scheduler
- Business rule group
- Mediation
- Recovery
- Relationship service
- Selector
- Event Sequencing (Lock Manager)
- Enterprise Service Bus Logger Mediation Primitive
- Messaging Engines (if you select the **Use this database for Messaging Engines (MEs)**)

The Common Event Infrastructure component uses the Common Event Infrastructure database.

For more information about the various databases and database tables the WebSphere Process Server product uses, see Choosing a database.

Important: If you choose Derby Network Server or Derby Network Server 40 as your database product, ensure that the server is running on the host and port you specified during profile creation or augmentation, even if the database host is local. You can make sure that the server is running only after the profile is created or augmented.

a. In the **Choose a database product** field, select the database product you want to use, or accept the default value of Derby Embedded or Derby Embedded 40 (for stand-alone server profiles) or Derby Network Server or Derby Network Server 40 (for deployment manager profiles).

   Restriction: Informix Dynamic Server and Microsoft SQL Server are not supported on deployment managers using the deployment environment configuration.

b. To store the database creation and configuration scripts that the profile creation or augmentation process creates in a location other than the default location, select the **Override the destination directory for generated scripts** check box and designate your new location in the **Database script output directory** field. The profile creation or augmentation process creates scripts that you or the database administrator can run manually to create new databases and their required tables, if you choose not to do so during profile creation or augmentation. The process creates scripts for the Common database for all profile types and scripts for the Common Event Infrastructure database for stand-alone server profiles.

   The default locations for the databases are as follows:

   - For the Common Event Infrastructure database:

     – ` Linux ` ` UNIX ` *install_root*/profiles/*profile name*/dbscripts/CEI_*ceiDbName*

     – ` Windows ` *install_root*\profiles*profile name*\dbscripts\CEI_*ceiDbName*

   - For the Common database:

     – ` Linux ` ` UNIX ` *install_root*/profiles/*profile name*/dbscripts/CommonDB/*dbType*/*dbName*

     – ` Windows ` *install_root*\profiles*profile name*\dbscripts\CommonDB*dbType**dbName*

For selected database products, you can prevent automatic creation and configuration of databases by selecting the **Delay execution of database scripts (must select if using a remote database)**.)

c. Enter your Common database name or accept the default value.

The name of the database on IBM i using Independent Auxiliary Storage Pools (IASPs) can be the name of the IASP.

Default Common database names differ based on the database product:

- *SYSBAS for DB2 for i5/OS (Toolbox) and DB2 for iSeries® i (Toolbox)
- WPRCSDB for all other database products

If you plan to use an existing database, this name must match the name of that database. If you plan to create a new database and the name you specify is already associated with another WebSphere Process Server profile, you must use a different database name.

Note: This restriction does not apply to IBM i. All profiles on IBM i use the same database name.

Note: The Oracle database name (dbName) is the Oracle Identifier (SID) and must exist in order to create tables. When creating stand-alone server profiles, it can be shared between the Common database and the Common Event Infrastructure database. It is recommended that you remove all Oracle database resources before creating a new profile, because the Common Event Infrastructure database creates unique database resources, such as table spaces, which will fail if they exist in the Oracle server.

d. Select the **Delay execution of database scripts (must select if using a remote database)** check box if you do not want to create and configure a local database automatically or create tables in an existing one during profile creation or augmentation. A local database will be created if this check box is not selected.

By selecting **Delay execution of database scripts (must select if using a remote database)**, you or the database administrator must manually run the scripts that are stored in the location specified in the **Database script output directory** field on this page.

Restriction: The **Delay execution of database scripts (must select if using a remote database)** option is not available for the following configurations:

- If you chose the Derby Embedded, Derby Embedded 40, Derby Network Server, or Derby Network Server 40 product for any profile type.
- If you chose to create a deployment manager using the Deployment environment option.

For more information about the various databases and database tables the WebSphere Process Server product uses, see Choosing a database.

Important: If you choose Derby Network Server or Derby Network Server 40 as your database product, ensure that the server is running on the host and port you specified during profile creation or augmentation, even if the database host is local. You can make sure that the server is running only after the profile is created or augmented.
.

See the following topics for instructions on manually creating and configuring databases:

- To create a new Common database or create tables in an existing one, see "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417.

Important: Do not use the Common database scripts located in the following directories (where the variable *db_type* represents the supported database product):

- Linux UNIX *install_root*/dbscripts/CommonDB/*db_type*
- Windows *install_root*\dbscripts\CommonDB*db_type*

These default scripts have not been updated by the profile creation or augmentation process.

Restriction: The **Delay execution of database scripts (must select if using a remote database)** option is not available for the following configurations:

- If you chose the Derby Embedded, Derby Embedded 40, Derby Network Server, or Derby Network Server 40 product for any profile type.
- If you chose to create a deployment manager using the Deployment environment option.

e. Click **Next** to display the Database Configuration (Part 2) page.

The page displays with fields specific to the database product that you have selected. The page prompts you for database-specific information. It contains slightly different fields and default values, depending on your database product selection.

You must complete this page even if you chose to postpone creating a new database or adding tables to an existing one by selecting the Delay execution of database scripts check box on the previous Database Configuration page. The values you choose on the Database Configuration (Part 2) page are added to the database configuration scripts stored in the directory you specified in the Database script output directory field on the previous page (or in the default directory for these scripts if you did not specify a different location).

Restriction: You cannot create a new database if you are using DB2 for z/OS V8 or V9, or Oracle. In these cases, the Common database and, for a stand-alone server profile, the Common Event Infrastructure database, must exist. If you select one of these databases, a warning message alerts you to this restriction.

When you have completed the Database Configuration (Part 2) page, click **Next**. The tool checks that a valid connection exists to the Common database. If the tool identifies an error, you must correct the problem before continuing by either making sure that the database is up and running or altering parameters in order to make a good connection.

Derby Embedded or Derby Embedded 40

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select Derby Embedded or Derby Embedded 40 as your database product.

Important: If you choose Derby Embedded or Derby Embedded 40 as your database product, after profile creation or augmentation completes, ensure that the server is running on the host and port you specified during profile creation, even if the database host is local.

Table 40. Required database configuration fields for Derby Embedded or Derby Embedded 40

Field	Action needed
Schema name	Enter the database schema name. Default is APP.

Derby Network Server or Derby Network Server 40

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select Derby Network Server or Derby Network Server 40 as your database product.

Important: If you choose Derby Network Server or Derby Network Server 40 as your database product, after profile creation or augmentation completes, ensure that the server is running on the host and port you specified during profile creation, even if the database host is local.

Table 41. Required database configuration fields for Derby Network Server or Derby Network Server 40

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1527 or enter the correct server port number.
Schema name	Enter the database schema name. Default is APP.

DB2 Universal Database

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 Universal Database as your database product.

Table 42. Required database configuration fields for DB2 Universal Database

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.

Table 42. Required database configuration fields for DB2 Universal Database (continued)

Field	Action needed
Location (directory) of JDBC driver classpath files	Accept the default value of `install_root`/universalDriver_wbi/lib on Linux and UNIX platforms, or `install_root`\universalDriver_wbi\lib on Windows platforms, or browse to the location on your system that contains the following files: • db2jcc.jar • db2jcc_license_cu.jar *or* db2jcc_license_cisuz.jar An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 50000 or enter the correct server port number.
Schema name	Enter the database schema name. Default is WPRCDB.

DB2 Data Server

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 Data Server as your database product.

Table 43. Required database configuration fields for DB2 Data Server

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `install_root`/universalDriver_wbi/lib on Linux and UNIX platforms, or `install_root`\universalDriver_wbi\lib on Windows platforms, or browse to the location on your system that contains the following files: • db2jcc.jar • db2jcc_license_cu.jar *or* db2jcc_license_cisuz.jar An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 50000 or enter the correct server port number.
Schema name	Enter the database schema name. Default is WPRCDB.

DB2 for z/OS V8 and V9

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 for z/OS V8 and V9 as your database product. You cannot create a new database using these databases. The Common database and, for a stand-alone server profile, the Common Event Infrastructure database, must exist.

Table 44. Required database configuration fields for DB2 for z/OS V8 and V9

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • `db2jcc.jar` • `db2jcc_license_cisuz.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Enter the database server host name.
Server port	Accept the default value of `446` or enter the correct server port number.
Database alias name	Enter the database alias name.
Connection location	Enter the connection location.
Storage group name	Enter the storage group name.

DB2 for i5/OS (Toolbox) and DB2 for IBM i (Toolbox)

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select or DB2 for IBM i (Toolbox) as your database product. This selection is also valid for DB2 for i5/OS (Toolbox).

Table 45. Required database configuration fields for DB2 for IBM i (Toolbox) or DB2 for IBM i (Toolbox)

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `/QIBM/ProdData/HTTP/Public/jt400/lib` or browse to the location on your system that contains the following file: • `jt400.jar` An error message is displayed if the file cannot be found at the specified location.
Database server host name (for example IP address)	Enter the database server host name.

Field	Action needed
Database collection name	Accept the default value of WPRCSDB or enter the correct schema name. To prevent naming conflicts within the specified database, specify a schema name whose first three characters are unique from the names of other schemas residing in the database.

Informix Dynamic Server

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select Informix Dynamic Server as your database product.

Table 46. Required database configuration fields for Informix Dynamic Server

Field	Action needed
Directory of database server installation	Indicates the database installation directory if you are using Informix databases.
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • ifxjdbc.jar • ifxjdbcx.jar An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of localhost or enter the correct database server host name.
Server port	Accept the default value of 1526 or enter the correct server port number.
Instance name	Enter the correct instance name.

Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft)

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select Microsoft SQL Server (DataDirect) or Microsoft SQL Server (Microsoft) as your database product.

Table 47. Required database configuration fields for Microsoft SQL Server DataDirect and Microsoft SQL Server (Microsoft)

Field	Action needed
CEI database user name	Enter the CEI database user name.
CEI database password	Enter a password to authenticate with the CEI database.
Confirm password	Confirm the password.
Common database user name	Enter the user name to authenticate with the database.

Field	Action needed
Common database password	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • sqlserver.jar • base.jar • util.jar Also, the file spy.jar must be available in the following location relative to the location of the JDBC driver class path files: • [Linux] [UNIX] ../spy/spy.jar • [Windows] ..\spy\spy.jar An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of localhost or enter the correct database server host name.
Database server name	Enter the database server name.
Server port	Accept the default value of 1433 or enter the correct server port number.
Admin user name	Enter the user ID that has privileges to create and drop databases and users or accept the default value of sa. This ID is required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Password	Enter the password for the user **Admin user name** ID.
Confirm password	Confirm the password.

Oracle

The following table lists the fields you must complete on the Database Configuration (Part 2) page when you select Oracle as your database product. You cannot create a new database using this database.

Important: You must have a user ID that has SYSDBA privileges before creating any profile.

Table 48. Required database configuration fields for Oracle

Field	Action needed
Directory of database server installation	Enter or browse for the database server installation. Required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Business Space database user name	User ID for the Business Space database. This option only appears if BSpace is enabled.

Table 48. Required database configuration fields for Oracle (continued)

Field	Action needed
Business Space database password	Enter a password to authenticate with the Business Space database.
Confirm password	Confirm the password.
CEI database user name	User ID for the Common Event Infrastructure database.
CEI database password	Enter a password to authenticate with the Common Event Infrastructure database.
Confirm password	Confirm the password.
Common database user name	User ID for the Common database.
Password	Enter a password to authenticate with the Common database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the file `ojdbc6.jar`. You must install the `ojdbc6.jar` driver to access the Oracle database. **Important:** Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle Web site. An error message is displayed if the files cannot be found at the specified location.
JDBC driver type	Click **OCI** or **Thin**.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1521 or enter the correct server port number.
System administrator user name	Enter the user ID that has privileges to create and drop databases and users or accept the default value of SYSUSER. Required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Password	Enter the password for the user **Admin user name** ID.
Confirm password	Confirm the password.

If you selected **Use this database for Messaging Engines (MEs)** in the first Database Configuration screen, the Database Configuration (Part 3) page displays. The following table lists the fields you must complete.

Table 49. Required database configuration fields for using Oracle with Messaging Engines

Field	Action needed
Business Process Choreographer messaging engine	
User name	Enter the Business Process Choreographer messaging engine user ID. This option only appears if BPC is enabled.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.

Field	Action needed
CEI bus messaging engine	
User name	Enter the CEI bus messaging engine user ID.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
SCA application bus messaging engine	
User name	Enter the SCA application bus messaging engine user ID.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
SCA system bus messaging engine	
User name	Enter the SCA system bus messaging engine user ID.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.

    f. Click **Next** to display the Profile Summary page.

16. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

17. Complete the profile configuration by doing one of the following tasks, depending on whether you must manually configure the Common database.

   - Because you decided to postpone database configuration by producing scripts to be run manually, perform the following steps:

     a. Clear the check box beside **Launch the First steps console** and click **Finish** to close the Profile Management Tool. Also, close the Profiles page, which is open in a separate window.

     b. Use your site's standard database definition tools and procedures to edit and run the scripts the Profile Management Tool generated to create or create and configure the WPRCSDB database (or its equivalent if it has a different name on your system).

       The default locations for the database scripts are as follows:

       – For the Common Event Infrastructure database:

         - `Linux` `UNIX` *install_root*/profiles/*profile name*/dbscripts/CEI_*ceiDbName*

         - `Windows` *install_root*\profiles*profile name*\dbscripts\ CEI_*ceiDbName*

       – For the Common database:

         - `Linux` `UNIX` *install_root*/profiles/*profile name*/dbscripts/CommonDB/*dbType*/*dbName*

         - `Windows` *install_root*\profiles*profile name*\dbscripts\ CommonDB*dbType**dbName*

       Also see *Creating the Common database and tables after profile creation or augmentation* for task descriptions on creating a new Common database or tables in an existing Common database.

Results

You have created a deployment manager profile and you have run the database configuration scripts to create Common database and tables.

What to do next

Start the deployment manager

Start the deployment manager

The deployment manager is a server process. You must start the deployment manager before you can use its administrative console to manage the cell.

Before you begin

You have created the deployment manager profile.

About this task

Perform the following steps to start and stop a deployment manager.

Procedure

1. Start the deployment manager with one of the following actions:
   - Windows From the **Start** menu, select **IBM WebSphere** → **Process Server 7.0** → **Profiles** → *profile_name* → **Start the deployment manager**.
   - In the First steps console, click **Start the deployment manager**.
   - Use the startManager command.
2. Verify that the deployment manager started successfully by checking the `install_root`/profiles/`profile_name`/logs/`server_name`/startServer.log log file for the message Server `server_name` open for e-business; process id is `nnnn`.

What to do next

Create the custom profiles

Creating Advanced custom profiles (managed nodes)

Selecting the Advanced option creates profiles with customized configuration settings.

Before you begin

You have created the deployment manager profile and you have run the database configuration scripts to create Common database and tables.

The Deployment manager is running.

About this task

While configuring custom profiles, you can specify your own values for settings such as ports, the location of the profile, and the names for the profile, node, host, and cell (if applicable). You can choose to federate the node to an existing deployment manager during the creation process, or federate it later using the addNode command.

Perform the following steps to create advanced custom profiles (managed nodes).

Procedure

1. Start the WebSphere Process Server Profile Management Tool.

   Use one of the following commands:

   - `Linux` `UNIX` *install_root*/bin/ProfileManagement/pmt.sh

   - `Windows` *install_root*\bin\ProfileManagement\pmt.bat

   The Welcome page is displayed.

2. In the Welcome page, click the **Launch Profile Management Tool** button or the **Profile Management Tool** tab.

   The **Profiles** tab is displayed.

3. In the **Profiles** tab, click **Create**.

   The **Profiles** tab can contain a list of profiles that have been created on your machine. For this procedure, it is assumed you are creating a new profile, not augmenting an existing one.

   The Environment Selection page opens in a separate window.

4. In the Environment Selection page, expand WebSphere Enterprise Service Bus or WebSphere Process Server and select the type of profile you want to create. Then click **Next**

   The Profile Creation Options page is displayed.

5. In the Profile Creation Options page, choose to perform an **Advanced** profile creation, and click **Next** to display the Optional Application Deployment page.

   The **Advanced** option lets you specify your own configuration values for a profile.

   By selecting the **Advanced** option, you can do the following:
   - Assign customized values to ports, to the location of the profile, and to the names of the profile, node, host, and cell (when applicable).
   - Configure the Common database.
   - Deploy the administrative console.
   - Enable administrative security.
   - Create a system service to run the server, if your operating system and the privileges of your user account permit the creation of services.

6. In the Profile Name and Location page, perform the following steps:

   a. Specify a unique name and directory path for the profile, or accept the defaults.

      Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name.

      The directory you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. The default directory is dependent on platform:

      - `Linux` `UNIX` *install_root*/profiles/*profile_name*

      - `Windows` *install_root*\profiles*profile_name*

      where *profile_name* is the name you specified. An error message is displayed if:
      - The *profile_name* you specify is not unique.
      - The directory you specify is not empty.
      - Your user ID does not have sufficient permissions for the directory.
      - There is insufficient space to create the profile.

b. You can make the profile you are creating the default profile (so commands work automatically with it) by selecting the **Make this profile the default** check box. This check box appears only if you have an existing profile on your system.

The first profile that you create on a machine is the default profile.

The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies. See "Profile commands in a multiprofile environment" on page 139 for more information.

The Profile Management Tool detects ports currently used by other WebSphere products, but not the ports of other applications that might use specified ports. When federating a custom profile, the addNode command uses non-conflicting ports. This action means that you can take the default port assignments as you create the profile, and let the addNode command specify non-conflicting ports as you federate the node. Port assignments must be unique on a server. Server processes on different servers can use the same port assignments without conflict.

c. Click **Next**. (If you click **Back** and change the name of the profile, you might have to manually change the name on this page when it is displayed again.)

The Node and Host Names page is displayed.

7. In the Node and Host Names page, specify the node and host names for the profile, or accept the defaults and click **Next**. Try to keep the node name as short as possible, but ensure that node names are unique within the deployment environment. See "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and other issues you must consider when naming.

The Federation page is displayed.

8. In the Federation page, select the **Federate this node later** check box and click **Next**

After you create the custom profiles you will federate the nodes using the addNode command.

How to decide whether or not to federate the node as part of custom profile creation:

Important:

Do *not* federate the custom node during profile creation if any one of the following situations is true:

- You plan to use this custom node as a migration target.
- Another profile is being federated. (Node federation must be serialized.)
- The deployment manager is not running or you are not sure if it is running.
- The deployment manager has not yet been augmented into a WebSphere Process Server deployment manager.
- The deployment manager is not at a release level the same or higher than the release level of the profile you are creating.
- The deployment manager does not have a JMX administrative port enabled.
- The deployment manager is re-configured to use the non-default remote method invocation (RMI) as the preferred Java Management Extensions (JMX) connector. (Select **System administration > Deployment manager >**

Administration services in the administrative console of the deployment manager to verify the preferred connector type.)

Processing associated with federating the node as part of custom profile creation:

- The Profile Management Tool verifies that the deployment manager exists and can be contacted, and that the authentication user ID and password are valid for that deployment manager (if it is secured).
- If you attempt to federate a custom node when the deployment manager is not running or is not available for other reasons, a warning box prevents you from continuing. If this warning box appears, click **OK** to exit from it, and then make different selections on the Federation page.

The Security Certificate (Part 1) page is displayed.

9. In the Security Certificate (Part 1) page, create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

The Security Certificate (Part 2) page is displayed.

10. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are:

- `key.p12`: Contains the default personal certificate.
- `trust.p12`: Contains the signer certificate from the default root certificate.
- `root-key.p12`: Contains the root signing certificate.
- `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
- `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
- `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify.

An imported certificate is added to the `key.p12` file or the `root-key.p12` file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

The next step depends on whether you elected to federate the profile as part of the profile creation process.

Because you chose not to federate the node as part of the custom profile creation, the Database Configuration page displays.

11. In the Database Configuration page, perform the following steps:

    a. Review the database product. The database that matches the database used on the deployment manager to which this custom profile will be federated is displayed.

    b. Provide the location (directory) of the JDBC driver class path files for the database. You can accept the default values for Derby Network Server, Derby Network Server 40 or DB2 Universal Database.

    c. Click **Next**.

    The Profile Summary page is displayed.

12. In the Profile Summary page, click **Create** to create the profile, or **Back** to change the characteristics of the profile.

    When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

    Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:

    • **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.

    • **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

    The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

13. In the Profile Complete page, clear the checkbox for **Launch the First steps console** and click **Finish** to close the Profile Management Tool. Also, close the Profiles page, which is open in a separate window.

What to do next

Repeat the steps you just completed to create a second custom profile for node 2.

After you have created the second custom profile, you must federate the nodes using the addNode command.

Federate the nodes

You can use the addNode command to federate a custom node into a deployment manager cell.

Before you begin

Before using this procedure, ensure that the following prerequisites are met:

- You have installed WebSphere Process Server and created a WebSphere Process Server deployment manager and two custom profiles. This procedure assumes you did *not* federate the custom profiles during its creation or augmentation, either with the Profile Management Tool or with the manageprofiles command-line utility.
- The deployment manager is running. If it is not, start it either by selecting **Start the deployment manager** from its First steps console or by entering the following command, where *profile_root* represents the installation location of the deployment manager profile:
  - `Linux` `UNIX` *profile_root*`/bin/startManager.sh`
  - `Windows` *profile_root*`\bin\startManager.bat`
- The deployment manager has been augmented into a WebSphere Process Server deployment manager. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.
- The deployment manager is at the same release level or higher than the custom profile you created or augmented.
- The deployment manager has a JMX administrative port enabled. The default protocol is SOAP.
- You do not plan to use this custom node as a migration target.

Avoid trouble: `Vista` `Windows 7` If you are installing the product on these operating systems, you must disable IPv6 and restart the machine to view and log on to the administrative console. See IPv6 for Microsoft® Windows®: Frequently Asked Questions for more information on disabling IPv6.

About this task

The following instructions guide you through the process of using the addNode command to federate and deploy custom nodes.

Run this command for each of the custom nodes (profiles) that you created in the previous tasks.

Procedure

1. Go to the `bin` directory of the custom profile you want to federate. Open a command window and go to one of the following directories (from a command line), depending on platform (where *profile_root* represents the installation location of the custom profile):
   - `Linux` `UNIX` *profile_root*`/bin`
   - `Windows` *profile_root*`\bin`
2. Issue the addNode command.

   Issue one of the following commands from the command line if security is not enabled:
   - `Linux` `UNIX` `./addNode.sh` *deployment_manager_host deployment_manager_SOAP_port*
   - `Windows` `addNode.bat` *deployment_manager_host deployment_manager_SOAP_port*

Issue one of the following commands from the command line if security is enabled:

- `Linux` `UNIX` `./addNode.sh` *deployment_manager_host* *deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication*

- `Windows` `addNode.bat` *deployment_manager_host* *deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication*

An output window opens. If you see a message similar to the following message, your custom profile was federated successfully:

`ADMU0003I: Node DMNDID2Node03 has been successfully federated.`

Results

You now have configured a cell with 1 deployment manager and two nodes.

What to do next

Now you are ready to Create the deployment environment for your ND configuration.

Create the deployment environment

Using the deployment environment configuration wizard create a network deployment pattern based on the remote messaging and remote support pattern.

Before you begin

Required security role for this task: When security and role-based authorization are enabled, you must log in to the administrative console as an administrator or operator to perform this task.

About this task

This task creates a deployment environment that is based on a specific pattern and uses the Deployment Environment Configuration wizard.

Procedure

1. From the administrative console, go to the Deployment Environments page by clicking **Servers** → **Deployment Environments** .

2. Launch the Deployment Environment Configuration wizard by clicking **New** on the Deployment Environments page.

   a. The **Create a deployment environment based on a pattern** option is selected. **Create a deployment environment based on a pattern** is the system default and it is the option described in this topic.

      Deployment environment patterns capture commonly used business integration topologies. A pattern provides you with a template for the deployment environment that you are creating.

      Note: Patterns have a direct relationship to the products supported by the configured deployment manager. WebSphere Process Server supports a specific set of patterns, with the *Remote messaging and remote support* pattern being the system default. If your deployment manager supports other products in addition to WebSphere Process Server, additional

patterns may apply. Consult product-specific documentation for information on patterns as they apply to the products.

For information on the types patterns included with and supported by WebSphere Process Server, see Topology types and deployment environment patterns in the Planning section.

See Custom deployment environment layout configuration for information on using the Custom Deployment Topology Detail page to configure your custom deployment environment.

b. Enter a unique name for the deployment environment in the **Deployment environment name** field.

c. **Optional:** To view all of the configuration steps in the wizard, select **Detailed: Show all steps**.

If you choose **Fast path: Show only needed steps** the wizard displays only those pages that **do not** have assigned default values. Choose **Fast path: Show only needed steps** only if you are agreeable to accepting the system-provided default values for the deployment environment configuration.

This topic assumes that you have chosen **Detailed: Show all steps**

d. Click **Next** to display the Deployment Environment Features page.

3. On the Deployment Environment Features page, select the feature for the deployment environment and click **Next** to either view a list of compatible features, or to view a list of deployment environment patterns. Features represent the runtime processing capabilities of your deployment environment.

The list of available features on the Deployment Environment Features page is based on the deployment manager profile. If your deployment manager profile has been augmented to include other products alongside WebSphere Process Server (for example, WebSphere Business Monitor or WebSphere Business Services Fabric), then the Deployment Environment Features page also lists these features.

If you have installed and configured a profile for WebSphere Process Server, then the Deployment Environment Features page includes the following:

- **WESB**, for WebSphere Enterprise Service Bus, which provides a deployment environment that supports mediations.
- **WPS**, for WebSphere Process Server, which provides a deployment environment that supports mediations, business processes, human tasks, and business rules.

The default value for the deployment environment feature matches the runtime capabilities of your deployment manager.

4. On the Select compatible deployment environment features page, select additional features as necessary and click **Next** to view the list of patterns associated with your primary and ancillary feature selections.

Note: The Select compatible deployment environment features page is displayed only if the deployment manager has been augmented with other business process management (BPM) features, such as WebSphere Business Monitor.

For an understanding of the relationship of features and compatible features, see the information on deployment environments in the Planning section.

5. On the Select the deployment environment pattern page, select the pattern for the selected deployment environment, then click **Next** to display the Select Nodes page.

The list of patterns that display on the Deployment Environment Patterns page is dynamic. This list is activated by, and dependent on, the following environment conditions and configuration decisions:

- The platform on which you have installed the software
- The selections that you have made on the Select the deployment environment feature page and the Select compatible deployment environment features page.

For a detailed description of the relationship of patterns to features, see Topology patterns and supported BPM product features

6. Optional: On the Select Nodes page, select the nodes that you want to include in this deployment environment, then click **Next** to display the Clusters page.

   Select at least one node for the deployment environment. For high-availability and failover environments, select at least two nodes. For scalability, select all nodes.

   To include a node, select the check box next to the node name. Use **Node Mapping** to map the selected node to another node name.

7. Optional: On the Clusters page, assign the required number of cluster members on each node for each cluster *type* (Application Deployment Target, Messaging Infrastructure and Supporting Infrastructure) of the deployment environment.

   By default one cluster member is assigned on each node for each function. You change the number by replacing the number in each column. If you are unfamiliar with the different cluster roles and functions provided by each type of cluster, see "Topology types and deployment environment patterns."

   A 0 (zero) value for a node means that the node does not contribute to the selected function, based on features that you have selected.

   After assigning cluster members, you can click **Next** to display the Cluster naming pages for each cluster type of the deployment environment. The Cluster naming sub-steps that display will vary depending on the deployment environment pattern selected.

   The system generates default values for cluster names and cluster member names.

   If you do not want to customize cluster names or cluster member names, you can use the wizard navigation pane to go directly to the REST Services page in a following step.

   Each substep page is structured in the same fashion, and is described in Customize the cluster names and cluster member names.

   a. Optional:

      Use the Cluster Naming page to customize cluster names or cluster member names for the cluster type. There is one substep page for each cluster *type* in the pattern that you have selected. For example, if you selected a **Remote messaging and remote support pattern**, there are 3 sub-steps, one for each type of cluster (Application Deployment Target, Messaging Infrastructure and Supporting Infrastructure) in that pattern.

      The information on each substep page is as follows:

      Cluster
      A read-only field specifying the functional role of the cluster.

      The value varies depending on the cluster type, as follows:

      - Application Deployment Target
      - Supporting Infrastructure

- Messaging Infrastructure

  For information on the functional role provided by each cluster type, see Topologies and deployment environment patterns

Cluster Name
Contains the system-generated default value for the cluster name.

Cluster Member Name
Accept the system-generated default value or specify a name of your choosing.

The default value for the cluster member name is based on the following naming convention: `<cluster name>.<node name>.<node number sequence>` .

The number of cluster member names that display in the table match the number of cluster members that you entered for the cluster type column and node row on the Clusters page. See the preceding step for the Clusters page.

8. On the REST Services page, configure service endpoints for Representational State Transfer (REST) application programming interfaces (APIs).

   If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets.

   a. Configure a full URL path for all REST services by selecting either **https://** or **http://** from the **Protocol** list.

   b. Enter a name in the **Host Name or Virtual Host in a Load-Balanced Environment** field.

   c. In the **Port** field, enter the port that a client needs to communicate with the server or cluster.

   d. In the table of REST services, if you want to modify the description of the REST service endpoint, overtype the entry in the Description field. The other fields are read-only.

   e. Click **Next** to go to the Import the database configuration page.

9. Optional: On the Import the database configuration page, click **Browse** to go the database design document or enter the path to the database design document and then click **Next** to go to the Data sources page. The design document can be based on a database design that you created using the database design tool (DDT), or it can be the supplied design document based on the pattern and feature that you have selected.

   Note: The database design document that you import for the deployment environment does not change the commonDB created at Profile Creation time.

10. Conditional optional: Database page, configure the database parameters for data sources of the deployment environment, then click **Next** to go to the Security page.

    On this page, define the database information for the components that are included in this deployment environment. Where possible, the wizard supplies default information for the parameters, but change those values to match the values that you defined when you planned the environment.

    Note: If you imported a database design document, the information on the Database page reflects the data source configuration as it exists in the database design document that you imported.

Whether or not this step displays for a fast path deployment environment configuration is conditional. This step displays for a fast path deployment environment configuration if more than one database has been defined.

This step always displays if you are using DB2 for z/OS or an Oracle database provider.

The default schema names that are displayed on this page might conflict with your site naming convention or might conflict with existing schemas. As such, it is likely that you will need to change the schema name.

Oracle database considerations:

- If you do not want to provide a DBA user name and password for all components when using Oracle, clear **Create tables** and specify preexisting and unique user names and passwords for each component. If you are able to provide a DBA user name and password for all the components, select **Create tables** and allow the configuration process to create the required schemas and users.

For a production environment, you should set the same values for **User name** and **Schema name** and you should deselect **Create tables**. For a production environment, create the required schemas manually and use the SQL files generated to create the tables.

Note: You cannot select **Create tables** for Business Space (the option is unavailable for selection). The SQL files for Business Space need to be run manually. For information on running the SQL manually for Business Space, see *Configuring Business Space database tables*.

You can edit all key parameters, such as the database name, whether or not to create tables, the data source runtime user name, and the password for the deployment environment.

You can select which database to use for the given component.

DB2 for z/OS: The **Create tables** option cannot be used if you are using a DB2 for z/OS database provider.

Steps that cannot be completed through the Deployment Environment Configuration wizard, and which need to be completed manually, are listed on the Deferred Configuration page.

11. On the Security page, configure the authentication aliases WebSphere uses when accessing secure components

    You can change the authentication alias user name and password on this page. These aliases are used to access secure components but do not provide access to data sources

12. On the Business Process Choreographer page, set parameters for the Business Process Choreographer configuration and then click **Next** to display the System web applications page. On this page you specify the values for:

    - Security roles
    - Authentication aliases

13. Optional: On the System web applications page, set the context root for component-based web applications in your deployment environment or accept the system-provided default values for the context roots. Then click **Next** to display the Summary page.

    The System web applications page displays for deployment environments using the Remote messaging, support and web applications pattern. The Remote messaging, support and web applications pattern applies if the deployment environment is for a deployment manager that has been augmented to include WebSphere Business Monitor.

The table contains the following control information.

Web Application
The name of the Web application.

Some of the components that are part of the deployment environment you are creating contain web applications. The **Web application** column can include the following components:

- Business Space
- Business Process Choreographer Explorer
- Business Rules Manager

Context Root
The current value of the context root for the component.

By default, the default context root for the web application applies. You can change the context roots by typing over the value in the **Context Root** field.

Note: The Business Space context root is read only and cannot be edited.

14. Verify that the information on the Summary page is correct and click **Finish and Generate Environment** to save and complete the configuration of the deployment environment. To exit without completing the configuration, click **Finish**.

Clicking **Finish** saves the deployment environment configuration - but does not generate it.

Click **Cancel** cancels the deployment configuration and does not save the configuration.

a. Check for deferred configuration steps

Select **Deployment Environments** → *name of deployment environment* → **Deferred Configuration**

You need to address any existing deferred configuration steps before starting the Deployment Environment.

Configuring profiles

There are three types of profiles: a stand-alone server profile, a deployment manager profile (a management profile with a deployment manager server), and a custom profile (managed node). Each profile defines a separate runtime environment, with separate files (commands, configuration files, and log files). Topics in this section provide detailed information about tasks you might have to perform to work with profiles after you install WebSphere Process Server.

Profiles

A profile defines a unique runtime environment, with separate command files, configuration files, and log files. Profiles define three different types of environments on WebSphere Process Server systems: stand-alone server, deployment manager, and managed node.

Using profiles, you can have more than one runtime environment on a system, without having to install multiple copies of the WebSphere Process Server binary files.

Use the Profile Management Tool or the manageprofiles command-line utility to create profiles.

Note: On distributed platforms, each profile has a unique name. On the z/OS platform, all profiles are named "default".

The profile directory

Every profile in the system has its own directory containing all of its files. You specify the location of the profile directory when you create the profile. By default, it is in the `profiles` directory in the directory where WebSphere Process Server is installed. For example, the Dmgr01 profile is in `C:\Program Files\IBM\WebSphere\ ProcServer\profiles\Dmgr01`.

The First steps console

Every profile in the system has a First steps console. You can use this interface to familiarize yourself with the stand-alone server, deployment manager, or managed node.

The default profile

The first profile that you create within one installation of WebSphere Process Server is the *default profile*. The default profile is the default target for commands issued from the `bin` directory in the directory where WebSphere Process Server was installed. If only one profile exists on a system, every command operates on that profile. If you create another profile, you can make it the default.

Note: The default profile is not necessarily a profile whose name is "default".

Augmenting profiles

If you already have a deployment manager profile, a custom profile, or a stand-alone server profile created for WebSphere Application Server Network Deployment or WebSphere ESB, you can *augment* it to support WebSphere Process Server in addition to existing function. To augment a profile, first install WebSphere Process Server. Then use the Profile Management Tool or the manageprofiles command-line utility.

Restriction: You cannot augment a profile if it defines a managed node that is already federated to a deployment manager.

Prerequisites for creating or augmenting profiles

Before creating or augmenting a profile, you must ensure that a series of prerequisites have been met.

- You must have an existing installation of WebSphere Process Server. If you do not, see "Installing the software" on page 41 for installation procedures.
- If you are not the user ID who installed the product, you must have write permission to selected directories within the WebSphere Process Server installation. See "Granting write permission of files and directories to nonroot users for profile creation" on page 193 for instructions on how to obtain these permissions. You must create your profiles in a directory other than *install_root*/profiles.
- You must know the type of profile you want to create or augment. For more information about profiles, see "Profiles" on page 188.
- You must follow the correct procedure to create or augment the profile:

- If you want to create a new profile rather than augment an existing profile, see one of the following topics:
  - To create a profile using an interactive interface: "Creating profiles using the Profile Management Tool" on page 197.
  - To create a profile using the manageprofiles command-line utility: "Creating profiles using the manageprofiles command-line utility" on page 253.
- If you want to augment an existing WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus profile into a WebSphere Process Server profile, see one of the following topics:
  - To augment a profile using an interactive interface: "Augmenting profiles using the Profile Management Tool" on page 301.
  - To augment a profile using the manageprofiles command-line utility: "Augmenting profiles using the manageprofiles command-line utility" on page 340.

  Important: A profile that you plan to augment cannot define a managed node that is already federated.

- You cannot use the Profile Management Tool to create or augment profiles on WebSphere Process Server installations on 64-bit architectures except on the Linux on zSeries platform. To create or augment profiles on other 64-bit architectures, you can use the manageprofiles command-line utility. For information about using the manageprofiles command-line utility, see "Creating profiles using the manageprofiles command-line utility" on page 253 and "Augmenting profiles using the manageprofiles command-line utility" on page 340. You can also use the Profile Management Tool on these architectures if you use a WebSphere Process Server 32-bit installation.
- You must shut down any servers associated with a profile you plan to augment.
- You must review "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and issues that you must consider when naming your profile, node, host, server (if applicable), and cell (if applicable).
- You must have enough disk and temporary space to create or augment the new profile. For information about space requirements, see WebSphere Process Server detailed system requirements at http://www.ibm.com/support/docview.wss?uid=swg27006205 and select the link to your version of WebSphere Process Server.

The following prerequisites relate to product databases:
- During the profile creation or augmentation process, you are configuring the database used by the Common Event Infrastructure component and the Common database used by other selected components. Whether you plan to create new databases and tables or postpone actual database configuration by producing scripts that must be run manually by you or your database administrator (DBA), you must know the database details listed in the following topics:
  - "manageprofiles parameters for Common Event Infrastructure database configuration (per database product)" on page 291
  - "manageprofiles parameters for Common database configuration (per database product)" on page 280
- If you plan to use Oracle as your database product, you must have a user ID that has SYSDBA privileges before creating any profile.

- If you plan to use or create the Common database repository on a remote server, you must create it before beginning to create or augment the profile. You can create a repository on the local server or use an existing one on a remote server. See "Creating the Common database manually before product installation" on page 31 for the location of default scripts you can use to create this database.
- If you plan to use DB2 on a remote z/OS workstation for the Common Event Infrastructure and Common database repositories, your DBA must create, on the z/OS server, three databases called `event`, `eventcat`, and `WPRCSDB`, as well as the correct storage groups for each (`EVTSTO` is the default). The DBA can use the site's standard database definition tools and procedures.

  Before running CreateDB.sh, you must allocate the following buffer pools with these DB2 commands:

  ```
  -ALTER BUFFERPOOL (BP1) VPSIZE(20000)
  -ALTER BUFFERPOOL (BP2) VPSIZE(20000)
  -ALTER BUFFERPOOL (BP3) VPSIZE(20000)
  ```

  You must also make sure that permission to use them has been granted as follows:

  ```
  GRANT USE OF BUFFERPOOL BP1 TO PUBLIC;
  GRANT USE OF BUFFERPOOL BP2 TO PUBLIC;
  GRANT USE OF BUFFERPOOL BP3 TO PUBLIC;
  ```

  - To create the `event` and `eventcat` databases and associated storage groups, the DBA can reference Configuring the event database and its subtopics.
  - To create the `WPRCSDB` database and associated storage groups, the DBA can edit and run the default scripts provided in the following directories:
    - `Linux` `UNIX` *install_root*/dbscripts/CommonDB/DB2zOSV8/ or *install_root*/dbscripts/CommonDB/DB2zOSV9/
    - `Windows` *install_root*\dbscripts\CommonDB\DB2zOSV8\ or *install_root*\dbscripts\CommonDB\DB2zOSV9\

- Database administrator (DBA) privileges are required for the database configuration panels that are part of creating a deployment manager profile. If you plan to use the deployment environment feature of the Profile Management Tool and want to use a database other than Derby Network Server as your database product, the user ID you provide for the **User name to authenticate with the database field** on the database configuration panels must have DBA privileges.

  The user ID requires DBA privileges even if you elect to postpone database creation during the installation or profile creation procedure, because electing to postpone database creation prevents creation of the Common database only. When the Profile Management Tool configures a deployment environment (clustered topology), it also creates the required tables and schemas on the backend database server for the Business Process Choreographer, the Common Event Infrastructure, and the messaging engines, in addition to the Common database. The user ID must have DBA privileges so that these schemas and tables can be created without database permission errors.

  If the user ID does not have DBA privileges, use this workaround:

  1. Install the product without creating a profile.
  2. Use the Profile Management Tool to create the deployment manager and the custom profiles using the Advanced path for all. Do not use the Typical or Deployment environment paths. Select the option to delay the execution of the database scripts during deployment manager profile creation.

3. Have the DBA create the Common DB. The information at the following site provides the necessary scripts to manually create database objects: "Creating the Common database and tables after profile creation or augmentation" on page 416.

4. Federate the custom profiles to the deployment manager.

5. Using the administrative console, create the required deployment environment. See "Creating a deployment environment using a pattern" on page 446 for more information.

- `Linux` `UNIX` If you plan to use DB2 Universal Database:

You must run the db2profile script to set the required DB2 environment that is used to invoke the DB2 commands, which are used during profile creation. Add the db2profile script to the `/etc/profile` directory:

`vi /etc/profile and add below lines:`

```
export PATH=/opt/IBM/db2/V9.5/bin:$PATH
. /home/db2inst1/sqllib/db2profile
```

You must add the user ID that will be used during profile creation to the DB2 administrative groups. For example, if you log in as the root user and are creating the database using db2inst1 as the user ID, add the root to the `/etc/group` administrative groups:

`vi /etc/group and update below lines:`

```
dasadm:|;101:dasusr1,db2inst1,root
db2iadm:|:102;root
db2fadm:|:103;db2fenc1,root
```

Typical profile creation Exceptions:

When the db2profile script is not run:

```
/opt/HJJ/wps4013/util/dbUtils/profileHelpers/commonDBUtility.ant:841: Execute failed:
java.io.IOException: Cannot run program "db2" (in directory "/opt/HJJ/
wps4013/profiles/Dmgr01/dbscripts/CommonDB/DB2/WPSDB1")
```

When the DB2 database manager is not running:

```
SQL1032N No start database manager command was issued. SQLSTATE=57019
```

When the user who installed WebSphere Process Server and is creating the profile is not added to the DB2 administrative groups:

```
SQL1092N "ROOT" does not have the authority to perform the requested command.

When DB2 database mananger is down or not running...

SQL1032N  No start database manager command was issued.  SQLSTATE=57019
```

- If you plan to use Derby Network Server, you must start the Derby Network Server before creating or augmenting profiles.

Starting the Derby Network Server:

`WAS_HOME/derby/bin/networkServer/startNetworkServer.sh|bat -h dbHostName -p dbServerPort`

For example: `startNetworkServer.sh -h myHost.ibm.com -p 1567`

Note: The `profilePath/properties/commondb.properties` file contains the host name and port values that were used during WebSphere Process Server profile creation.

If Derby Network Server is not running during profile creation, it will start automatically. For example, if WebSphere Process Server does not find Derby Network Server listening on the specified port, it will be started automatically. When profile creation is complete, Derby Network Server will automatically be stopped.

If the server is not started, the components that attempt to use the database will log the following exceptions in the `systemout.log`:

```
WSVR0501E: Error creating component null [class com.ibm.wbiserver.commondb.
admin.CommonDBComponentImpl]com.ibm.ws.exception.RuntimeWarning:
Database is not configured or not available.
```

```
CWSTM0004E: The connection to the data source with a JNDI name of jdbc/WPSDB that
is used to hold business rules and selectors failed as it may not have been created
or it is unreachable.
```

- If you plan to use Microsoft SQL Server 2005 with a standalone profile, and will put the messaging engine tables in the Common Database, then you must perform the following steps:

  1. Manually add four schemas to the Common database before creating stand-alone server profiles. These schemas are *XXX*SS00, *XXX*SA00, *XXX*CM00, and *XXX*BM00, where *XXX* is the first three characters of the name of the Common database.

  2. Pass the `dbCommonForME=true` parameter during profile creation. The following command configures the Messaging Engines on SQL Server with the schemas that were defined above. The command uses the `dbUserId` and `dbPassword` that you specified for CommonDB.

     ```
     C:\WebSphereND\bin\manageprofiles.bat" -create -templatePath "C:\WebSphereND\
     profileTemplates\default.wbiserver" -dbHostName LNIDDBTUMSQL21 -
     dbServerPort 1433 -dbDelayConfig
     true -configureBSpace true -ceiDbName EVENT  -dbType MSSQLSERVER_Microsoft -
     dbUserId
     wpcdbadmin -dbJDBCClasspath "C:\Program Files\Microsoft SQL Server\JDBC\
     sqljdbc_1.2\enu"
     -dbName WPRCSDB -dbPassword qlwiddj23 -ceiDbServerName LNIDDBTUMSQL21 -dbCommonForME=true
     ```

- To configure network deployment environments, refer to the following technote: General instructions for creating deployment environments with Microsoft SQL Server Enterprise 2005.

After you have reviewed these prerequisites, return to the topic from which you accessed this one.

Granting write permission of files and directories to nonroot users for profile creation

The product installer (who can be a root/Administrator or nonroot user) can grant write permission to the appropriate WebSphere Process Server files and directories to nonroot users. The nonroot users can then create profiles. Alternatively, the product installer can create a group for users who are authorized to create profiles or give individual users the authority to create profiles. The following example task shows how to create a group that is authorized to create profiles.

Throughout this text, the terms "installer" and "product installer" refer to the user ID that installed WebSphere Process Server.

Restriction: WebSphere Process Server does not support changing ownership of existing profiles from the product installer to nonroot users. Thus, profile augmentation by nonroot users of profiles owned by another user is not supported.

Nonroot users create their own profiles so that they can manage their own environments. Typically, they manage environments for development purposes.

Nonroot users must store their profiles in their private directory structure, not in the *install_root*/profiles directory of the product.

Restriction: An ease-of-use limitation exists for nonroot users who create profiles. Mechanisms within the Profile Management Tool that suggest unique names and port values are disabled for nonroot users. The nonroot user must change the default field values in the Profile Management Tool for the profile name, node name, cell name, and port assignments. The product installer can assign nonroot users a range of values for each of the fields, and assign responsibility to the nonroot users for adhering to their assigned value ranges and for maintaining the integrity of their own definitions.

If you already created at least one profile, then certain directories and files were created. Because these directories and files were created, skip the steps in this topic that create these directories and files. If no profile was previously created, then you must complete the steps to create the required directories and files. In most cases, a profile has been created previously.

Steps the product installer must perform to grant appropriate permissions

The installer can perform the following steps to create the `profilers` group and give the group appropriate permissions to create a profile.

1. Log on to the WebSphere Process Server system as the product installer. (The product installer can be a root/Administrator or nonroot user.)
2. Using operating system commands, perform the following steps:
   - Create a group named profilers, which will contain all users who can create profiles.
   - Create a user named user1, who can create profiles.
   - Add users product_installer and user1 to the profilers group.
3. `Linux` `UNIX` Log off and log back on as the installer to pick up the new group.
4. Create the following directories as the installer if no profile exists:
   - `Linux` `UNIX` Create the *install_root*/logs/manageprofiles directory:

     `mkdir install_root/logs/manageprofiles`

     `Windows` Create the *install_root*\logs\manageprofiles directory by following instructions in the Windows documentation. For this example procedure, the directory is:

     `install_root\logs\manageprofiles`
   - `Linux` `UNIX` Create the *install_root*/properties/fsdb directory:

     `mkdir install_root/properties/fsdb`

     `Windows` Create the *install_root*\properties\fsdb directory by following instructions in the Windows documentation. For this example procedure, the directory is:

     `install_root\properties\fsdb`
5. As the installer, follow directions for your operating system to create the profileRegistry.xml file if no profile exists. For this example, the file paths are:

   `Linux` `UNIX`

   `install_root/properties/profileRegistry.xml`

   `Windows`

   `install_root\properties\profileRegistry.xml`

Follow instructions for your operating system to add the following information to the profileRegistry.xml file. The file must be encoded as UTF-8.

```
<?xml version="1.0" encoding="UTF-8"?>
<profiles/>
```

6. As the product installer, use operating system tools to change directory and file permissions.

   Linux **UNIX** The following example assumes that the variable $WASHOME is the WebSphere Process Server root installation directory /opt/IBM/WebSphere/ProcServer.

```
export WASHOME=/opt/IBM/WebSphere/ProcServer
echo $WASHOME
echo "Performing chggrp/chmod per WAS directions..."
chgrp profilers $WASHOME/logs/manageprofiles
chmod g+wr  $WASHOME/logs/manageprofiles
chgrp profilers $WASHOME/properties
chmod g+wr  $WASHOME/properties
chgrp profilers $WASHOME/properties/fsdb
chmod g+wr  $WASHOME/properties/fsdb
chgrp profilers $WASHOME/properties/profileRegistry.xml
chmod g+wr  $WASHOME/properties/profileRegistry.xml
chgrp -R profilers $WASHOME/profileTemplates
```

   HP-UX Issue the following additional command where *profile_template_name* is default, dmgr, or managed:

```
chmod -R g+wr $WASHOME/profileTemplates/profile_template_name/documents
```

   HP-UX The ownership of files is preserved when the files are copied to the profile directory during profile creation. You granted write permission to the profile directory so that files copied to the profile directory can be modified as part of the profile creation process. Files that are already in the profileTemplates directory structure before the start of profile creation are not modified during profile creation.

   Linux Issue the following additional commands:

```
chgrp profilers $WASHOME/properties/Profiles.menu
chmod  g+wr $WASHOME/properties/Profiles.menu
```

   Windows The following example assumes that the variable $WASHOME is the WebSphere Process Server root installation directory C:\Program Files\IBM\WebSphere\ProcServer. Follow instructions in the Windows documentation to give the profilers group read and write permission to the following directories and their files:

```
@WASHOME\logs\manageprofiles
@WASHOME\properties
@WASHOME\properties\fsdb
@WASHOME\properties\profileRegistry.xml
```

   You might have to change the permissions on additional files if the nonroot user encounters permission errors. For example, if the product installer authorizes a nonroot user to delete a profile, then the product installer might have to delete the following file:

   Linux **UNIX** *install_root*/properties/profileRegistry.xml_LOCK

   Windows *install_root*\properties\profileRegistry.xml_LOCK

   Give write access to the nonroot user for the file to authorize the user to delete the file. If the nonroot user still cannot delete the profile, then the product installer can delete the profile.

Result

The installer created the `profilers` group and gave the group proper permissions
to certain directories and files to create profiles. These directories and files are the
only ones in the installation root of WebSphere Process Server to which a nonroot
user needs to write to create profiles.

What to do next

The nonroot user that belongs to the `profilers` group can create profiles in a
directory that the nonroot user owns and to which the nonroot user has write
permission. However, the nonroot user cannot create profiles in the installation
root directory of the product.

A nonroot user ID can manage multiple profiles. The same nonroot user ID can
manage an entire profile, whether it is the deployment manager profile, a profile
that contains the servers and the node agent, or a custom profile. A different user
ID can be used for each profile in a cell, whether global security or administrative
security is enabled or disabled. The user IDs can be a mix of root and nonroot user
IDs. For example, the root user might manage the deployment manager profile,
while a nonroot user might manage a profile that contains servers and the node
agent, or vice versa. However, typically, a root user or a nonroot user can manage
all profiles in a cell.

The nonroot user can use the same tasks to manage a profile that the root user
uses.

Creating profiles

You can create new WebSphere Enterprise Service Bus or WebSphere Process
Server profiles interactively by using the Profile Management Tool graphical user
interface (GUI) or from a command line by using the manageprofiles
command-line utility.

Before you begin

- Choose the type of profile you want to create. For more information about
  profiles, see "Profiles" on page 188.
- See the list of prerequisites for creating or augmenting profiles in the topic
  "Prerequisites for creating or augmenting profiles" on page 189.

About this task

You can create any combination of deployment manager, stand-alone server, or
custom profiles. Each time you use the Profile Management Tool or manageprofiles
command-line utility, you create one profile.

Restriction:

You cannot use the Profile Management Tool to create profiles on WebSphere
Process Server installations on 64-bit architectures except on the Linux on zSeries
platform. To create profiles on other 64-bit architectures, you can use the
manageprofiles command-line utility. For information about using the
manageprofiles command-line utility, see "Creating profiles using the
manageprofiles command-line utility" on page 253. You can also use the Profile
Management Tool on these architectures if you use a WebSphere Process Server
32-bit installation.

Procedure

Decide whether to create the profile interactively by using the Profile Management Tool, or from a command line by using the manageprofiles command-line utility.

- To create the profile by using the Profile Management Tool, see the topic "Creating profiles using the Profile Management Tool."
- To create the profile by using the manageprofiles command-line utility, see the topic "Creating profiles using the manageprofiles command-line utility" on page 253.

Creating profiles using the Profile Management Tool

Use the Profile Management Tool graphical user interface (GUI) to create a stand-alone server profile, a deployment manager profile, or a custom profile.

Before you begin

- Review the list of prerequisites for creating or augmenting profiles at "Prerequisites for creating or augmenting profiles" on page 189.

- Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons. To fix the problem, add the following lines to the *install_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before starting the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

Procedure

1. Start the WebSphere Process Server Profile Management Tool.

   Use one of the following commands:

   - Linux UNIX *install_root*/bin/ProfileManagement/pmt.sh

   - Windows *install_root*\bin\ProfileManagement\pmt.bat

   See the topic "Starting the Profile Management Tool" on page 199 for other methods of starting this tool.

   The Welcome page is displayed.

2. In the Welcome page, click the **Launch Profile Management Tool** button or the **Profile Management Tool** tab.

   The **Profiles** tab is displayed.

3. In the **Profiles** tab, click **Create**.

   The **Profiles** tab can contain a list of profiles that have been created on your machine. For this procedure, it is assumed you are creating a new profile, not augmenting an existing one. If you want to augment an existing version 7.0 profile, see the topic "Augmenting profiles using the Profile Management Tool" on page 301.

   The Environment Selection page opens in a separate window.

4. In the Environment Selection page, expand WebSphere Enterprise Service Bus or WebSphere Process Server and select the type of profile you want to create. Then click **Next**.

   You can also create WebSphere Application Server profiles with this Profile Management Tool. However, this documentation addresses creating WebSphere Enterprise Service Bus or WebSphere Process Server profiles only.

The Profile Creation Options page is displayed.

5. In the Profile Creation Options page, choose to perform a **Typical**, an **Advanced**, or (for deployment manager or custom profiles) a **Deployment environment** profile creation, and click **Next**.

   The **Typical** option creates a profile with default configuration settings.

   The **Advanced** option lets you specify your own configuration values for a profile.

   The **Deployment environment** option also lets you specify your own configuration values for a profile, plus lets you create a deployment manager and choose a deployment environment pattern for it or choose a cluster or clusters to apply to a managed node.

6. Before continuing to the next page in the Profile Management Tool, proceed to one of the following topics to configure and complete creation of your profile.

Type of profile creation you selected	Procedure to complete profile creation based on your profile type (stand-alone server, deployment manager, or custom)
Typical	• "Creating **Typical** stand-alone server profiles" on page 200 • "Creating **Typical** deployment manager profiles" on page 212 • "Creating **Typical** custom profiles (managed nodes)" on page 226
Advanced	• "Creating **Advanced** stand-alone server profiles" on page 202 • "Creating **Advanced** deployment manager profiles" on page 214 • "Creating **Advanced** custom profiles (managed nodes)" on page 229

Type of profile creation you selected	Procedure to complete profile creation based on your profile type (stand-alone server, deployment manager, or custom)
Deployment environment **Important:** If you do not have an existing deployment manager and deployment environment pattern, be sure to follow the instructions under "Creating Deployment environment deployment manager profiles" on page 220 when creating profiles on your first workstation. Follow the instructions under "Creating **Deployment environment** custom profiles (managed nodes)" on page 235 when creating profiles on subsequent workstations. **Note:** If you are using Microsoft SQL Server (DataDirect) or Microsoft SQL Server (Microsoft), use the administrative console to configure another database type for Business Process Choreographer and Business Space. **Restriction:** Database administrator (DBA) privileges are required for the database configuration panels that are part of creating a deployment manager profile. If you plan to use the deployment environment feature of the Profile Management Tool and want to use a database other than Derby Network Server as your database product, the user ID you provide for the **User name to authenticate with the database field** on the database configuration panels must have DBA privileges.	• "Creating Deployment environment deployment manager profiles" on page 220 • "Creating **Deployment environment** custom profiles (managed nodes)" on page 235

Results

You are ready to configure your profile, which defines a new operating environment of the type you specified (stand-alone server, deployment manager, or custom).

Starting the Profile Management Tool:

Before you start the Profile Management Tool, be aware of the restrictions and ensure that certain prerequisites are met. You can start the Profile Management Tool in several ways, depending on the platform on which it is running.

Restrictions:
• You cannot use the Profile Management Tool to create or augment profiles on WebSphere Process Server installations on 64-bit architectures except on the Linux on zSeries platform. To create profiles on other 64-bit architectures, you can use the manageprofiles command-line utility. For information about using the manageprofiles command-line utility, see "Creating profiles using the manageprofiles command-line utility" on page 253. You can also use the Profile Management Tool on these architectures if you use a WebSphere Process Server 32-bit installation.

- **`Vista`** **`Windows 7`** **Restriction for nonadministrative users with multiple instances:** If you install multiple instances of WebSphere Process Server as the root user and give a nonadministrative user access to only a subset of those instances, the Profile Management Tool does not function correctly for the nonadministrative user. In addition, a `com.ibm.wsspi.profile.WSProfileException` or `Access is denied` message occurs in the `install_root\bin\ProfileManagement\pmt.bat` file. By default, nonadministrative users do not have access to the `Program Files` directory, which is the default installation location for the product. To resolve this issue, nonadministrative users can install the product or be given permission to access the other product instances.

`Linux` **`UNIX`** **`Windows`** The language of the Profile Management Tool is determined by the default language on the system. If the default language is not one of the supported languages, then English is used. You can override the default language by starting the Profile Management Tool from the command line and using the `java user.language` setting to replace the default language. Run the following command:

- **`Linux`** **`UNIX`** `install_root/java/bin/java -Duser.language=locale install_root/bin/ProfileManagement/startup.jar`

- **`Windows`** `install_root\java\bin\java -Duser.language=locale install_root\bin\ProfileManagement\startup.jar`

For example, to start the Profile Management Tool in the German language on a Linux system, type the following command:

```
install_root/java/bin/java -Duser.language=de install_root/  \
bin/ProfileManagement/startup.jar
```

Starting the tool on all platforms

Start the tool on any platform from the First steps console. See "Starting the First steps console" on page 58 for how to start the First steps console.

Starting the tool on Linux and UNIX platforms

`Linux` **`UNIX`** You can start the tool on Linux and UNIX platforms by running the command `install_root/bin/ProfileManagement/pmt.sh`

`Linux` On Linux platforms only, you can also use operating system menus to start the Profile Management Tool. For example, click `Linux_operating_system_menus_to_access_programs` > `IBM WebSphere` > `your_product` > `Profile Management Tool`.

Starting the tool on Windows platforms

`Windows` You can use the following methods to start the tool on Windows platforms:
- Use the Windows Start menu. For example, select **Start > Programs *or* All Programs > IBM WebSphere > Process Server 7.0 > Profile Management Tool**.
- Run the command `install_root\bin\ProfileManagement\pmt.bat`

Creating Typical stand-alone server profiles:

Learn how to use the **Typical** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus stand-alone server profiles. Selecting the **Typical** option creates profiles with default configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a stand-alone server profile, and have selected the **Typical** profile creation option.

About this task

In this type of configuration, the Profile Management Tool does the following:
- Assigns default values to ports, to the location of the profile, and to the names of the profile, node, server, host, and cell.
- Installs the administrative console.
- Installs the default application (which contains the Snoop, Hello, and HitCount applications).
- Lets you optionally enable administrative security.
- Creates a personal security certificate for the profile. The certificate has a personal key and private key, each with a default value of WebAS (you must change this password). The expiration period is one year.
- Creates a root signing security certificate for signing other certificates. The certificate has a personal key and private key, each with a default value of WebAS (you must change this password). The expiration period is 15 years.
- If your operating system and the privileges of your user account permit, creates a system service to run the server.
- Sets the Common Event Infrastructure and Common database configurations to Derby Embedded.
- Configures Business Space powered by WebSphere using Derby Embedded.
- If you enable security, creates a sample Business Process Choreographer configuration for the profile. If you do not enable security, the sample configuration is not created.

Restriction: If you plan to federate the stand-alone server profile to a deployment manager, do not use the **Typical** option to create it. The default values for messaging engine storage and database type provided in a **Typical** profile creation are not suitable deployment environment installations. Use the **Advanced** option to create the profile instead. See "Creating **Advanced** stand-alone server profiles" on page 202 for instructions.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, you are viewing the Administrative Security page.

Procedure

1. Optionally enable administrative security.

   You can enable administrative security now, or later from the administrative console. To enable administrative security now, leave the **Enable administrative security** check box selected, supply a user name and password to log on to the administrative console, and click **Next**. To disable administrative security, clear

the check box. To enable administrative security later from the administrative console, open the console and select **Security > Business Integration Security**.

Important: If you want the Profile Management Tool to create a Business Process Choreographer sample configuration, you must enable administrative security.

The Profile Summary page is displayed.

2. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

   When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

   Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:
   - **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
   - **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

   The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

3. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to start the server.

Results

You have created a WebSphere Process Server or WebSphere Enterprise Service Bus profile. The node within the profile has a server named `server1` for Linux, UNIX, and Windows platforms and the number is incremented if there is more than one product installation.

What to do next

Check the server operation by selecting **Start the server** from the First steps console. An output window opens. If you see a message like the following one, your server is operating properly:

```
ADMU3000I: Server server1 open for e-business; process id is 3348
```

You can also check server operation by running the Installation Verification Test (IVT) from the First steps console or running the wbi_ivt command-line utility. This test is to verify that your deployment manager or stand-alone server installation is operating properly. For a stand-alone server profile, it also runs a System Health check and generates a report.

Creating Advanced stand-alone server profiles:

Learn how to use the **Advanced** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus stand-alone server profiles. Selecting the **Advanced** option creates profiles with customized configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a stand-alone server profile, and have selected the **Advanced** profile creation option.

About this task

By selecting the **Advanced** option, you can do the following:
- Assign customized values to ports, to the location of the profile, and to the names of the profile, node, server, host, and cell (when applicable).
- Configure the Common Event Infrastructure.
- Configure the Common database.
- Deploy the administrative console and the WebSphere Application Server sample application.
- Deploy the default application (which contains the Snoop, Hello, and HitCount Servlets).
- Create a Web server definition.
- Enable administrative security.
- Create a system service to run the server, if your operating system and the privileges of your user account permit the creation of services.
- Configure Business Space powered by WebSphere using Derby Embedded or Derby Embedded 40.
- Configure Business Rules Manager and create a Business Process Choreographer sample configuration.
- Configure the databases using a database design file.

Important: If you plan to federate the profile to a deployment manager, do not select the file store option for the messaging engines or Derby Embedded or Derby Embedded 40 for the Common Event Infrastructure, Business Process Choreographer, or Common databases. The file store option and Derby Embedded or Derby Embedded 40 database cannot be used in a deployment environment configuration.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, the Optional Application Deployment page is displayed.

Procedure

1. In the Optional Application Deployment page, select the applications that you want to deploy to the stand-alone server profile environment you are creating, then click **Next**.
    - **Deploy the Sample applications**: Installs the WebSphere Application Server sample applications. The WebSphere Application Server sample applications are not recommended for deployment to production environments.

      Note: The WebSphere Process Server Samples are *not* deployed when you select this check box.
    - **Deploy the administrative console (recommended)**: Installs a Web-based administrative console that manages the server.
    - **Deploy the default application**: Installs the default application that contains the Snoop, Hello, and HitCount Servlets.

The Profile Name and Location page is displayed.

2. In the Profile Name and Location page, perform the following steps.

   a. Specify a unique name and directory path for the profile, or accept the defaults.

   Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name. If you elect not to use the default name, see "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about issues you must consider when naming the profile, such as restrictions on the length of the directory name.

   The directory you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. The default directory is dependent on platform:

   - `Linux`   `UNIX`   *install_root*/profiles/*profile_name*
   - `Windows`   *install_root*\profiles*profile_name*

   where *profile_name* is the name you specified. An error message is displayed if:

   - The *profile_name* you specify is not unique.
   - The directory you specify is not empty.
   - Your user ID does not have sufficient permissions for the directory.
   - There is not sufficient space to create the profile.

   b. To create the stand-alone server with configuration settings optimized for development environments, select the **Create the server using the development template** check box. The development template reduces startup time and allows the server to run on less powerful hardware. Do not use this option for production servers.

   c. You can make the profile you are creating the default profile (so commands work automatically with it) by selecting the **Make this profile the default** check box. This check box appears only if you have an existing profile on your system.

   The first profile that you create on a workstation is the default profile.

   The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies. See "Profile commands in a multiprofile environment" on page 139 for more information.

   d. Click **Next**. (If you click **Back** and change the name of the profile, you might have to manually change the name on this page when it is displayed again.)

   The Node and Host Names page is displayed.

3. In the Node and Host Names page, specify the node, server, host, and cell names for the stand-alone server profile, or accept the defaults and click **Next**. Try to keep the node name as short as possible, but ensure that node names are unique within your deployment environment. See "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and other issues you must consider when naming.

   The Administrative Security page is displayed.

4. Optionally enable administrative security.

You can enable administrative security now, or later from the administrative console. To enable administrative security now, leave the **Enable administrative security** check box selected, supply a user name and password to log on to the administrative console, and click **Next**. To disable administrative security, clear the check box. To enable administrative security later from the administrative console, open the console and click **Security > Business Integration Security**.

Important: If you plan to create a Business Process Choreographer sample configuration in step 10 on page 208, you must enable administrative security.

If you chose to deploy the WebSphere Application Server sample application from the Optional Application Deployment page in step 1 on page 203, it requires an account under which to run. Supply the password for the account. You cannot change the user name of the account.

The Security Certificate (Part 1) page is displayed.

5. In the Security Certificate (Part 1) page, create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

The Security Certificate (Part 2) page is displayed.

6. In the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are:

- `key.p12`: Contains the default personal certificate.
- `trust.p12`: Contains the signer certificate from the default root certificate.
- `root-key.p12`: Contains the root signing certificate.
- `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
- `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
- `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify.

An imported certificate is added to the `key.p12` file or the `root-key.p12` file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

7. Verify that the ports specified for the profile are unique and click **Next**.

   The Profile Management Tool detects ports currently used by other WebSphere products and displays recommended port values that do not conflict with existing ones. If you have applications other than WebSphere ones that use specified ports, verify that the ports do not conflict. If you chose not to deploy the administrative console on the Optional Application Deployment page in step 1 on page 203, the administrative console ports are not available on the Port Values Assignment page.

   Ports are recognized as being in use if the following conditions are satisfied:
   - The ports are assigned to a profile created under an installation performed by the current user.
   - The ports are currently in use.

   Although the tool validates ports when you access the Port Values Assignment page, port conflicts can still occur resulting from selections you make on subsequent Profile Management Tool pages. Ports are not assigned until profile creation completes.

   If you suspect a port conflict, you can investigate it after the profile is created. Determine the ports used during profile creation by examining the following file:

   - Linux   UNIX   *profile_root*/properties/portdef.props
   - Windows   *profile_root*\properties\portdef.props

   Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in an existing profile in the WebSphere Application Server Network Deployment information center. Run the `updatePorts.ant` file through the ws_ant script detailed in this topic.

   The next step depends on your platform and whether you are installing as a root (Administrator) or nonroot user.

If you are installing	Next step
On a Linux or Windows platform, *and have root or Administrator group privileges*	The Linux or Windows Service Definition page is displayed. Proceed to step 8.
On any other platform or as a nonroot user on a Linux or Windows platform	The Web Server Definition page is displayed. Proceed to step 9 on page 207.

8. Linux   Windows   Choose whether to run the process as a Windows service on a Windows platform or as a Linux service on a Linux platform and click **Next**.

   Windows   The Windows Service Definition page is displayed for the Windows platform only if the ID that installs the Windows service has the Administrator group privilege. If the profile is configured as a Windows service, the product starts Windows services for processes started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Windows service and issue the startServer or startManager commands, the wasservice command starts the defined services.

Important: If you choose to log on as a specified user account, you must specify the user ID and the password for the user who is to run the service, and the startup type (default is `Manual`). The user ID must not have spaces in its name, it must belong to the Administrator group, and it must have the advanced user right "Log on as a service." If the user ID belongs to the Administrator group, the Profile Management Tool grants it the advanced user right if it does not already have it.

During profile deletion, you can remove the Windows service that is added during profile creation.

IPv6 considerations when running profiles as Windows services

Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as Local System. Create a user-specific environment variable to enable IPv6. Because this environment variable is a user variable instead of a Local System variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as Local System. When the WebSphere Process Server or WebSphere Enterprise Bus Windows service tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the WebSphere Process Server or WebSphere Enterprise Bus Windows service runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as Local System.

Linux The Linux Service Definition page is displayed only if the current operating system is a supported version of Linux and the current user has the appropriate permissions.

WebSphere Process Server attempts to start Linux services for processes that are started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Linux service and issue the startServer or startManager commands, the wasservice command starts the defined services.

By default, WebSphere Process Server is not selected to run as a Linux service.

To create the service, the user who runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, the Linux Service Definition page is not displayed, and no service is created.

You must specify a user name under which the service runs.

To delete a Linux service, the user must be the root user or have proper privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service on behalf of the user.

9. If you want to include a Web server definition in the profile now, perform the following steps:

    a. Select the **Create a Web server definition** check box.

    b. Specify the Web server characteristics on the page, and click **Next**.

    c. Specify the Web server characteristics on Part 2 of the page and click **Next**.

    If you use a Web server to route requests to WebSphere Process Server or WebSphere Enterprise Bus, you need to include a Web server definition. You can include the definition now, or define the Web server to WebSphere Process Server or WebSphere Enterprise Bus later. If you define the Web server definition during the creation of this profile, you can install the Web server and its plug-in after you create the profile. However, you must install both to the paths that you specify on the Web Server Definition pages. If you define

the Web server to WebSphere Process Server or WebSphere Enterprise Service Bus after you create this profile, you must define the Web server in a separate profile.

The Business Process Choreographer Configuration page is displayed.

10. Choose whether to create a Business Process Choreographer sample configuration.

    Restriction: Do not create a Business Process Choreographer sample configuration if you plan to use this component in a production environment or federate this stand-alone server profile to a deployment manager. The sample configuration is for development use only. For instructions on how to set up this component in a production setting, see the topics under Configuring Business Process Choreographer.

    To create a sample configuration, select the **Configure a sample Business Process Choreographer** check box and click **Next**.

    The Business Space Configuration page is displayed.

11. On the Business Space Configuration page, leave the **Configure Business Space** check box selected to set up Business Space powered by WebSphere, an integrated user experience for application users across the IBM WebSphere business process management portfolio. If you want to configure Lotus Webform Server to work with Human Task Management widgets in Business Space, select the **Configure Lotus Webform Server** check box and enter the Webform Server translator and installation root. Then click **Next**. Configuring Business Space sets up an integrated GUI for the business users of your application for this profile.

    Important: Business Space is supported with the following database products: Derby Embedded or Derby Embedded 40, Derby Network Server or Derby Network Server 40, DB2 Universal, DB2 for i5/OS (DB2 for IBM i), DB2 for z/OS, Oracle, and Microsoft SQL Server 2005 and 2008.

    If the database you use for WebSphere Process Server does not match the supported databases for Business Space, a Derby Embedded or Derby Embedded 40 database is selected for the Business Space configuration. You cannot federate this profile into a deployment environment later, because Derby Embedded or Derby Embedded 40 is not supported for deployment environments.

    The Business Rules Manager Configuration page is displayed.

12. Select whether to configure a Business Rules Manager for the installation and then click **Next**. Business Rules Manager is a Web application that customizes the business rules templates for your business application needs.

13. Optional: Configure the databases using a design file. This option is available for both Advanced stand-alone server and Advanced deployment manager profiles.

    a. Select **Use a database design file for database configuration**.

    b. Click **Browse**.

    c. Specify the fully qualified path name for the design file.

    d. Click **Next**.

    If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating the database design file using the database design tool" on page 431.

14. In the Database Configuration page, configure both the Common database and the database used by the Common Event Infrastructure component used by selected WebSphere Process Server and WebSphere Enterprise Bus components.

    Refer to the "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240 topic for details and return to this step when you have completed the fields on the Database Configuration page and the Database Configuration (Part 2) page.

    The Profile Summary page is displayed.

15. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

    When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

    Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:

    - **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
    - **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

    The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

16. Complete the stand-alone server profile configuration by performing one of the following tasks, depending on whether you must manually configure the Common Event Infrastructure and Common databases.

    - If you completed configuration of the Common Event Infrastructure and Common databases using the Profile Management Tool, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to start the server.
    - If you chose to postpone actual database configuration by producing scripts to be run manually, perform the following steps:

        a. Clear the check box beside **Launch the First steps console** and click **Finish** to close the Profile Management Tool. Also, close the Profiles page, which is open in a separate window.

        b. Use your site's standard database definition tools and procedures to edit and run the scripts the Profile Management Tool generated to create, or create and configure, the `event`, `eventcat`, and `WPRCSDB` databases (or their equivalents if they have different names on your system). You identified the location for these scripts in step 2 on page 241 of the topic "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240. Also see the topics that describe manually creating new databases or new tables in existing databases:

            – For the Common Event Infrastructure database: Configuring the event database and its subtopics.

            – For the Common database: "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417.

When the databases are configured, start the First steps console associated with the profile, as described in "Starting the First steps console" on page 58.

17. If you plan to use the Business Process Choreographer component in your environment, you might need your database administrator to create and configure the Business Process Choreographer database.

   For more information, see the topics under Configuring Business Process Choreographer.

Results

You have created a WebSphere Process Server or WebSphere Enterprise Service Bus profile. If you used the default server name, the node within the profile has a server named server1 on Linux, UNIX, and Windows platforms. The server number is incremented if there is more than one product installation.

What to do next

Check server operation by selecting **Start the server** from the First steps console. An output window opens. If you see a message like the following message, your server is operating properly:

```
ADMU3000I: Server server1 open for e-business; process id is 3348
```

You can also check server operation by running the Installation Verification Test (IVT) from the First steps console or running the wbi_ivt command-line utility. This test is to verify that your deployment manager or stand-alone server installation is operating properly. For a stand-alone server profile, it also runs a System Health check and generates a report.

Federating stand-alone server profiles to a deployment manager:

Learn how to use the **addNode** command to federate a stand-alone server profile into a deployment manager cell. After federation, a node agent process is created. Both this node agent and the server process are managed by the deployment manager. If you federate a stand-alone server profile and include all of its applications, the act of federation installs the applications on the deployment manager. A stand-alone server profile can be federated only if there are no other federated profiles.

Before you begin

Ensure that the following prerequisites are met:

- You have installed WebSphere Process Server and created a WebSphere Process Server deployment manager.
- The deployment manager has been augmented into a WebSphere Process Server deployment manager. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.
- The stand-alone server profile is a WebSphere Process Server profile.
- The stand-alone server profile does not use file store or Derby Embedded data store for its messaging engines. If you created the profile using the **Typical** option in the Profile Management Tool, the profile uses these options. You cannot federate it to a deployment manager.

- The stand-alone server uses a database driver that supports remote access, such as Derby Network or Java toolbox JDBC.
- The deployment manager is running. If it is not, start it either by selecting **Start the deployment manager** from its First steps console or by entering the following command, where *profile_root* represents the installation location of the deployment manager profile:
  - `Linux` `UNIX` *profile_root*`/bin/startManager.sh`
  - `Windows` *profile_root*`\bin\startManager.bat`
- The stand-alone server is *not* running. If it is, stop it either by selecting **Stop the server** from its First steps console or by entering the following command, where *profile_root* represents the installation location of the stand-alone server profile:
  - `Linux` `UNIX` *profile_root*`/bin/stopServer.sh`
  - `Windows` *profile_root*`\bin\stopServer.bat`
- The deployment manager is at the same release level or higher than the profile you created or augmented.
- The deployment manager has a JMX administrative port enabled. The default protocol is SOAP.
- No other nodes are federated to the deployment manager.

If you federate a stand-alone server profile when the deployment manager is not running or is not available for other reasons, profile federation fails and the resulting profile is unusable. You must then move this stand-alone server profile directory out of the profile repository before creating another profile with the same profile name.

About this task

Perform this task when you have an existing stand-alone server profile and you need to add the capabilities that network deployment offers to that server (central management or clustering). This function provides a growth path for an existing stand-alone server profile. However, you are limited to a single cluster configuration for this deployment environment. See Single cluster topology for a description of the single cluster pattern.

Perform this task once for each cell and only for the first profile federated to the cell. Do not perform this task if the cell already has federated nodes. When you create an environment where you do not have an existing stand-alone server profile, create the environment using custom profiles. See "Creating profiles" on page 196 for information about creating custom profiles.

Procedure

1. Go to the `bin` directory of the stand-alone server profile you want to federate. Open a command window and go to one of the following directories, depending on platform, where *profile_root* represents the installation location of the stand-alone server profile:
   - `Linux` `UNIX` *profile_root*`/bin`
   - `Windows` *profile_root*`\bin`
2. Issue the addNode command.

   Issue one of following commands if security is not enabled. The port parameter is optional and can be omitted if you used the default port numbers when creating the deployment manager profile:

- **`Linux`** **`UNIX`** `./addNode.sh` *deployment_manager_host deployment_manager_SOAP_port* `-includeapps -includebuses`

- **`Windows`** `addNode.bat` *deployment_manager_host deployment_manager_SOAP_port* `-includeapps -includebuses`

Issue one of the following commands if security is enabled:

- **`Linux`** **`UNIX`** `./addNode.sh` *deployment_manager_host deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication* `-localusername` *localuserID_for_authentication* `-localpassword` *localpassword_for_authentication* `-includeapps -includebuses`

- **`Windows`** `addNode.bat` *deployment_manager_host deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication* `-localusername` *localuserID_for_authentication* `-localpassword` *localpassword_for_authentication* `-includeapps -includebuses`

An output window opens. If you see a message like the following one, your stand-alone server profile was federated successfully:

```
ADMU0003I: Node DMNDID2Node02 has been successfully federated.
```

Results

The stand-alone server profile is federated into the deployment manager. For more information about the addNode command and its parameters, see the topic Using wsadmin scripting to run the addNode command in the WebSphere Application Server Network Deployment information center.

Creating Typical deployment manager profiles:

Learn how to use the **Typical** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus deployment manager profiles. Selecting the **Typical** option creates profiles with default configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a deployment manager profile, and have selected the **Typical** profile creation option.

About this task

In this type of configuration, the Profile Management Tool does the following:
- Assigns default values to ports, to the location of the profile, and to the names of the profile, node, host, and cell.
- Installs the administrative console.
- Lets you optionally enable administrative security.
- Creates a personal security certificate for the profile. The certificate has a personal key and private key, each with a default value of `WebAS` (you must change this password). The expiration period is one year.
- Creates a root signing security certificate for signing other certificates. The certificate has a personal key and private key, each with a default value of `WebAS` (you must change this password). The expiration period is 15 years.

- If your operating system and the privileges of your user account permit, creates a system service to run the server.
- Sets the Common database configuration to Derby Network Server.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, you are viewing the Administrative Security page.

Procedure

1. Optionally enable administrative security.

   You can enable administrative security now, or later from the administrative console. To enable administrative security now, leave the **Enable administrative security** check box selected, supply a user name and password to log on to the administrative console, and click **Next**. To disable administrative security, clear the check box. To enable administrative security later from the administrative console, open the console and click **Security > Business Integration Security**.

   The Profile Summary page is displayed.

2. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

   When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

   Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:

   - **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
   - **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

   The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

3. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console start the server.

4. If you plan to use the Business Process Choreographer component in your environment, you must configure it. You might need your DBA to create and configure the Business Process Choreographer database.

   For more information, see the topics under Configuring Business Process Choreographer.

Results

You have created a WebSphere Process Server or a Websphere Enterprise Service Bus profile.

The node defined by the profile has a deployment manager named Dmgr.

What to do next

Check the server operation by selecting **Start the deployment manager** from the First steps console. An output window opens. If you see a message like the following one, your deployment manager is operating properly:

```
ADMU3000I: Server dmgr open for e-business; process id is 3072
```

In a deployment environment, you must create and configure other databases, create custom profiles, and federate them to your deployment manager, create servers, create clusters if you want workload management capabilities, and perform other tasks specific to your planned installation environment. Your planned environment dictates which tasks you must perform and the order in which you perform them.

For more information about planning your installation, see the topics in the *Planning the Installation, version 7.0* PDF. To learn more about the databases required by WebSphere Process Server, see the topics under *Configuring WebSphere Process Server > Configuring databases* in the *Installing and Configuring WebSphere Process Server for Multiplatforms, version 7.0* PDF. Alternatively, view the topics in the WebSphere Process Server online information center.

Creating Advanced deployment manager profiles:

Learn how to use the **Advanced** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus deployment manager profiles. Selecting the **Advanced** option creates profiles with customized configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a deployment manager profile, and have selected the **Advanced** profile creation option.

About this task

By selecting the **Advanced** option, you can do the following:
- Assign customized values to ports, to the location of the profile, and to the names of the profile, node, host, and cell (when applicable).
- Configure the Common database.
- Deploy the administrative console.
- Enable administrative security.
- Create a system service to run the server, if your operating system and the privileges of your user account permit the creation of services.
- Configure the databases using a database design file.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, the Optional Application Deployment page is displayed.

Procedure
1. In the Optional Application Deployment page, select whether to deploy the administrative console to the profile environment you are creating, then click **Next**.

   The administrative console is a Web-based tool that manages the server. To choose to deploy the administrative console, leave the **Deploy the administrative console (recommended)** check box selected. Clear the check box to deselect it.

   The Profile Name and Location page is displayed.
2. In the Profile Name and Location page, perform the following steps.

a. Specify a unique name and directory path for the profile, or accept the defaults.

Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name. If you choose not to use the default name, see "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about issues you must consider when naming the profile, such as restrictions on the length of the directory name.

The directory you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. By default, this directory location is:

- `Linux` `UNIX` `install_root/profiles/profile_name`
- `Windows` `install_root\profiles\profile_name`

where *profile_name* is the name you specified. An error message is displayed if:

- The *profile_name* you specify is not unique.
- The directory you specify is not empty.
- Your user ID does not have sufficient permissions for the directory.
- There is insufficient space to create the profile.

b. You can make the profile that you are creating the default profile (so that commands work automatically with it) by selecting the **Make this profile the default** check box. This check box appears only if you have an existing profile on your system.

The first profile that you create on a workstation is the default profile.

The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies. See "Profile commands in a multiprofile environment" on page 139 for more information.

c. Click **Next**. (If you click **Back** and change the name of the profile, you might have to manually change the name on this page when it is displayed again.)

The Node, Host, and Cell Names page is displayed.

3. In the Node, Host, and Cell Names page, specify the node, host, and cell names for the deployment manager, or accept the defaults and click **Next**. Try to keep the node name as short as possible, but ensure that node names are unique within your deployment environment. See "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and other issues you must consider when naming.

The Administrative Security page is displayed.

4. Optionally enable administrative security.

You can enable administrative security now, or later from the administrative console. To enable administrative security now, leave the **Enable administrative security** check box selected, supply a user name and password to log on to the administrative console, and click **Next**. To disable administrative security, clear the check box. To enable administrative security later from the administrative console, open the console and select **Security > Business Integration Security**.

The Security Certificate (Part 1) page is displayed.

5. In the Security Certificate (Part 1) page, create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the `trust.p12` file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

The Security Certificate (Part 2) page is displayed.

6. In the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is `WebAS`. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the `java.security` file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are:

- `key.p12`: Contains the default personal certificate.
- `trust.p12`: Contains the signer certificate from the default root certificate.
- `root-key.p12`: Contains the root signing certificate.
- `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
- `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
- `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify.

An imported certificate is added to the `key.p12` file or the `root-key.p12` file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

7. Verify that the ports specified for the profile are unique and click **Next**.

The Profile Management Tool detects ports currently used by other WebSphere products and displays recommended port values that do not conflict with existing ones. If you have applications other than WebSphere ones that use specified ports, verify that the ports do not conflict. If you chose not to deploy the administrative console on the Optional Application Deployment page in step 1 on page 214, the administrative console ports are not available on the Port Values Assignment page.

Ports are recognized as being in use if the following conditions are satisfied:
- They are assigned to a profile created under an installation performed by the current user.
- They are currently in use.

Although the tool validates ports when you access the Port Values Assignment page, port conflicts can still occur resulting from selections you make on subsequent Profile Management Tool pages. Ports are not assigned until profile creation completes.

If you suspect a port conflict, you can investigate it after the profile is created. Determine the ports used during profile creation by examining the following file:

- `Linux` `UNIX` *profile_root*/properties/portdef.props
- `Windows` *profile_root*\properties\portdef.props

Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in an existing profile in the WebSphere Application Server Network Deployment information center. Run the `updatePorts.ant` file through the ws_ant script detailed in this topic.

The next step depends on your platform and whether you are installing as a root (Administrator) or nonroot user.

Installation type	Next step
On a Linux or Windows platform, *with root or Administrator group privileges*	The Linux or Windows Service Definition page is displayed. Proceed to step 8.
On any other platform, or as a nonroot user on a Linux or Windows platform	The Database Configuration page is displayed. Proceed to step 10 on page 218.

8. `Linux` `Windows` Choose whether to run the process as a Windows service on a Windows platform or as a Linux service on a Linux platform and click **Next**.

   `Windows` The Windows Service Definition page is displayed for the Windows platform only if the ID that installs the Windows service has the Administrator group privilege. If the profile is configured as a Windows service, the product starts Windows services for processes started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Windows service and issue the startServer or startManager commands, the wasservice command starts the defined services.

   Important: If you choose to log on as a specified user account, you must specify the user ID and the password for the user who is to run the service, and the startup type (default is `Manual`). The user ID must not have spaces in its name, it must belong to the Administrator group, and it must have the advanced user right "Log on as a service." If the user ID belongs to the Administrator group, the Profile Management Tool grants it the advanced user right if it does not already have it.

   During profile deletion, you can remove the Windows service that is added during profile creation.

   IPv6 considerations when running profiles as Windows services

   Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as Local System. Create a user-specific environment variable to enable IPv6. Because this environment variable is a user variable instead of a Local System variable, only a Windows service that

runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as Local System. When the WebSphere Process Server or WebSphere Enterprise Bus Windows service tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the WebSphere Process Server or WebSphere Enterprise Bus Windows service runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as Local System.

`Linux` The Linux Service Definition page is displayed only if the current operating system is a supported version of Linux and the current user has the appropriate permissions.

WebSphere Process Server attempts to start Linux services for processes that are started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Linux service and issue the startServer or startManager commands, the wasservice command starts the defined services.

By default, WebSphere Process Server is not selected to run as a Linux service.

To create the service, the user who runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, the Linux Service Definition page is not displayed, and no service is created.

You must specify a user name under which the service runs.

To delete a Linux service, the user must be the root user or have proper privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service on behalf of the user.

9. Optional: Configure the databases using a design file. This option is available for both Advanced stand-alone server and Advanced deployment manager profiles.

   a. Select **Use a database design file for database configuration**.
   b. Click **Browse**.
   c. Specify the fully qualified path name for the design file.
   d. Click **Next**.

   If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating the database design file using the database design tool" on page 431.

10. In the Database Configuration page, configure the Common database used by the selected product components.

    See the topic "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240 for details and return to this step when you have completed the fields on the Database Configuration and Database Configuration (Part 2) pages. The Profile Summary page is displayed.

11. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

    When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:

- **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
- **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

12. Complete the profile configuration by doing one of the following tasks, depending on whether you must manually configure the Common database.

- If you completed configuration of the Common database using the Profile Management Tool, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to start the deployment manager.
- If you decided to postpone actual database configuration by producing scripts to be run manually, perform the following steps:

   a. Clear the check box beside **Launch the First steps console** and click **Finish** to close the Profile Management Tool. Also, close the Profiles page, which is open in a separate window.

   b. Use your site's standard database definition tools and procedures to edit and run the scripts the Profile Management Tool generated to create or create and configure the WPRCSDB database (or its equivalent if it has a different name on your system). You identified the location for this script in step 2 on page 241 of the topic "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240. Also see the topics that describe manually creating a new Common database or tables in an existing Common database in "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417. When you have completed configuring the databases, start the First steps console associated with the profile, as instructed in "Starting the First steps console" on page 58.

Results

You created a WebSphere Process Server profile.

What to do next

Check server operation by selecting **Start the deployment manager** from the First steps console. An output window opens. If you see a message like the following one, your deployment manager is operating properly:

```
ADMU3000I: Server dmgr open for e-business; process id is 3072
```

In a deployment environment, you must create and configure other databases, create custom profiles, and federate them to your deployment manager, create servers, create clusters if you want workload management capabilities, and perform other tasks specific to your planned installation environment. Your planned environment dictates which tasks you must perform and the order in which you perform them.

For more information about planning your installation, see the topics in the *Planning the Installation, version 7.0* PDF. To learn more about the databases required by WebSphere Process Server, see the topics under *Configuring WebSphere Process Server > Configuring databases* in the *Installing and Configuring WebSphere Process Server for Multiplatforms, version 7.0* PDF. Alternatively, view the topics in the WebSphere Process Server online information center.

Creating Deployment environment deployment manager profiles:

Learn how to use the **Deployment environment** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus deployment manager profiles. Selecting the **Deployment environment** option lets you configure a profile with customized configuration values and use it in a new deployment environment based on a supplied pattern.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a deployment manager profile, and have selected the **Deployment environment** profile creation option.

About this task

Select the **Deployment environment** profile creation option to set up a fully configured profile for your deployment environment. This option configures and installs all components needed for WebSphere Process Server to work. The following components are configured as part of this option:
- Business Process Choreographer
- Common Event Infrastructure
- Business Rules Manager
- Service Component Architecture

In this type of configuration, you can do the following:
- Assign customized values to ports, to the location of the profile, and to the names of the profile, node, host, and cell (when applicable).
- Configure the Common database.
- Deploy the administrative console.
- Enable administrative security.
- Create a system service to run the server, if your operating system and the privileges of your user account permit the creation of services.
- Choose the deployment environment pattern to use.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, you are viewing the Profile Name and Location page.

Procedure

1. In the Profile Name and Location page, perform the following steps:
   - Specify a unique name and directory path for the profile, or accept the defaults.

     Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name.

The directory you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. By default, this directory location is:

–   `Linux`   `UNIX`   *install_root*/profiles/*profile_name*

–   `Windows`   *install_root*\profiles*profile_name*

where *profile_name* is the name you specified. An error message is displayed if:

–   The *profile_name* you specify is not unique.
–   The directory you specify is not empty.
–   Your user ID does not have sufficient permissions for the directory.
–   There is insufficient space to create the profile.

- You can make the profile that you are creating the default profile (so commands work automatically with it) by selecting the **Make this profile the default** check box. This check box appears only if you have an existing profile on your system.

  The first profile that you create on a workstation is the default profile.

  The default profile is the default target for commands that are issued from the bin directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies. See "Profile commands in a multiprofile environment" on page 139 for more information.

- Click **Next**. (If you click **Back** and change the name of the profile, you might have to manually change the name on this page when it is displayed again.)

  The Node, Host, and Cell Names page is displayed.

2. In the Node, Host, and Cell names page, specify the node, host, and cell names for the deployment manager, or accept the defaults and click **Next**. Try to keep the node name as short as possible, but ensure that node names are unique within the deployment environment. See "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and other issues you must consider when naming the node, host, and cell.

   The Administrative Security page is displayed.

3. Enable administrative security, Supply a user name and password to log on to the administrative console and click **Next**.

   Important: If you are performing a Deployment environment profile creation, administrative security is required.

   The Security Certificate (Part 1) page is displayed.

4. In the Security Certificate (Part 1) page, create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

   You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

   When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file. If you import the default personal certificate or the root signing

certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

The Security Certificate (Part 2) page is displayed.

5. In the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are:

- key.p12: Contains the default personal certificate.
- trust.p12: Contains the signer certificate from the default root certificate.
- root-key.p12: Contains the root signing certificate.
- default-signers.p12: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
- deleted.p12: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
- ltpa.jceks: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify.

An imported certificate is added to the key.p12 file or the root-key.p12 file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

6. Verify that the ports specified for the profile are unique and click **Next**.

The Profile Management Tool detects ports currently used by other WebSphere products and displays recommended port values that do not conflict with existing ones. If you have applications other than WebSphere ones that use specified ports, verify that the ports do not conflict.

Ports are recognized as being in use if the following conditions are satisfied:
- They are assigned to a profile created under an installation performed by the current user.
- They are currently in use.

Although the tool validates ports when you access the Port Values Assignment page, port conflicts can still occur resulting from selections you make on subsequent Profile Management Tool pages. Ports are not assigned until profile creation completes.

If you suspect a port conflict, you can investigate it after the profile is created. Determine the ports used during profile creation by examining the following file:

- **Linux** **UNIX** *profile_root*/properties/portdef.props

- **Windows** *profile_root*\properties\portdef.props

Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in an existing profile in the WebSphere Application Server Network Deployment information center. Run the updatePorts.ant file through the ws_ant script detailed in this topic.

The next step depends on your platform and whether you are installing as a root (Administrator) or nonroot user.

Installation Type	Next step
On a Linux or Windows platform, *and have root or Administrator group privileges*	The Linux or Windows Service Definition page is displayed. Proceed to step 7.
On any other platform, or as a non-root user on a Linux or Windows platform.	The Deployment Environment Configuration page is displayed. Proceed to step 8 on page 224.

7. **Linux** **Windows** Choose whether to run the process as a Windows service on a Windows platform or as a Linux service on a Linux platform and click **Next**.

    Windows The Windows Service Definition page is displayed for the Windows platform only if the ID that installs the Windows service has the Administrator group privilege. If the profile is configured as a Windows service, the product starts Windows services for processes started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Windows service and issue the startServer or startManager commands, the wasservice command starts the defined services.

    Important: If you choose to log on as a specified user account, you must specify the user ID and the password for the user who is to run the service, and the startup type (default is Manual). The user ID must not have spaces in its name, it must belong to the Administrator group, and it must have the advanced user right "Log on as a service." If the user ID belongs to the Administrator group, the Profile Management Tool grants it the advanced user right if it does not already have it.

    During profile deletion, you can remove the Windows service that is added during profile creation.

    IPv6 considerations when running profiles as Windows services

    Profiles created to run as a Windows service fail to start when using IPv6 if the service is configured to run as Local System. Create a user-specific environment variable to enable IPv6. Because this environment variable is a user variable instead of a Local System variable, only a Windows service that runs as that specific user can access this environment variable. By default, when a new profile is created and configured to run as a Windows service, the service is set to run as Local System. When the WebSphere Process Server or WebSphere Enterprise Bus Windows service tries to run, the service is unable to access the user environment variable that specifies IPv6, and thus tries to start as IPv4. The server does not start correctly in this case. To resolve the problem, when creating the profile, specify that the WebSphere Process Server or WebSphere Enterprise Bus Windows service runs as the same user ID under which the environment variable that specifies IPv6 is defined, instead of as Local System.

Linux The Linux Service Definition page is displayed only if the current operating system is a supported version of Linux and the current user has the appropriate permissions.

WebSphere Process Server attempts to start Linux services for processes that are started by the startServer or startManager commands. For example, if you configure a server or deployment manager as a Linux service and issue the startServer or startManager commands, the wasservice command starts the defined services.

By default, WebSphere Process Server is not selected to run as a Linux service.

To create the service, the user who runs the Profile Management Tool must be the root user. If you run the Profile Management Tool with a non-root user ID, the Linux Service Definition page is not displayed, and no service is created.

You must specify a user name under which the service runs.

To delete a Linux service, the user must be the root user or have proper privileges for deleting the service. Otherwise, a removal script is created that the root user can run to delete the service on behalf of the user.

8. In the Deployment Environment Configuration page, click the pattern to use for the deployment environment on this deployment manager profile.

Select the radio button beside one of the following patterns and click **Next**.

- **Remote Messaging and Remote Support** defines one cluster for the application deployment, one remote cluster for the messaging infrastructure, and one remote cluster for the Common Event Infrastructure and other supporting applications. This pattern configures a setup that performs well for most of your business integration needs. When in doubt, select this pattern.

- **Remote Messaging** defines one cluster for the application deployment and one remote cluster for the messaging infrastructure. The Common Event Infrastructure and other supporting applications are configured on the application deployment target cluster.

- **Single Cluster** defines one cluster for application deployment. Both messaging infrastructure and Common Event Infrastructure with supporting applications are configured on the application deployment cluster.

See the following topics for more information:

- Topology types and deployment environment patterns. A deployment environment pattern specifies the constraints and requirements of the components and resources involved in a deployment environment. The patterns are designed to meet the needs of most business requirements and are intended to help you create a deployment environment in the most straightforward way.

- Functions of IBM-supplied deployment environment patterns. To design a robust deployment environment, you need to understand the functionality each cluster can provide in a particular IBM-supplied deployment environment pattern or a custom deployment environment. This knowledge can help you make the correct decisions as to which deployment environment pattern best meets your needs.

The Database Configuration page is displayed.

9. In the Database Configuration page, configure the Common database used by all WebSphere Process Server components, including the Common Event Infrastructure database, the system bus messaging database, and all Business Process Choreographer-related databases.

If you want to use databases other than the Common one for these components, you have the following options:

- Cancel this deployment environment profile creation and instead create your deployment environment using the administrative console. See Creating deployment environments for more information.
- If you intend to use a different database product created by the same database vendor, you can still proceed with this profile creation and change the database configuration later in the administrative console. See Configuring a JDBC provider and data source in the WebSphere Application Server Network Deployment information center for more information about configuring JDBC drivers and data sources.

Refer to the topic "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240 for details and return to this step when you have completed the fields on the Database Configuration and Database Configuration (Part 2) information pages. The Profile Management Tool validates your database configuration selections and displays a message if any are in error. For example, if you enter a database name that exists and you are creating a new database, an error message informs you that the database exists.

Restriction:

Database administrator privileges are required for the database configuration panels that are part of creating a deployment manager profile for a deployment environment. If you plan to use the deployment environment feature, and want to use a database other than Derby Network Server as your database product, the user ID you provide for the "User name to authenticate with the database" field on the database configuration panels must have DBA privileges.

After you configure the Common database, the Profile Summary page is displayed.

10. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

   When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

   Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:
   - **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
   - **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

   The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

11. Complete the profile configuration by doing one of the following tasks, depending on whether you must manually configure the Common database.
   - If you completed configuration of the Common database using the Profile Management Tool, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to start the server.
   - If you decided to postpone database configuration by producing scripts to be run manually, perform the following steps:

a. Clear the check box beside **Launch the First steps console** and click **Finish** to close the Profile Management Tool. Also, close the Profiles page, which is open in a separate window.

b. Use your site's standard database definition tools and procedures to edit and run the scripts the Profile Management Tool generated to create or create and configure the WPRCSDB database (or its equivalent if it has a different name on your system). You identified the location for this script in step 2 on page 241 of the topic "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240. Also see the topics that describe manually creating a new Common database or tables in an existing one in "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417. When you have completed configuring the databases, start the First steps console associated with the profile, as instructed in "Starting the First steps console" on page 58.

Results

You have created a WebSphere Process Server or WebSphere Enterprise Bus profile.

The node within the profile has a deployment manager named dmgr.

What to do next

Ensure that your database instance is running before starting the deployment manager, even if the database is located locally. Then check server operation by selecting **Start the deployment manager** from the First steps console. An output window opens. If you see a message like the following one, your deployment manager is operating properly:

```
ADMU3000I: Server dmgr open for e-business; process id is 3072
```

Configure custom nodes in the deployment environment to complete the deployment environment pattern.

For more information about planning your installation, see the topics in the *Planning the Installation, version 7.0* PDF. To learn more about the databases required by WebSphere Process Server, see the topics under *Configuring WebSphere Process Server > Configuring databases* in the *Installing and Configuring WebSphere Process Server for Multiplatforms, version 7.0* PDF. Alternatively, view the topics in the WebSphere Process Server online information center.

Related tasks

"Setting up deployment environments" on page 445
Setting up deployment environments involves creating the deployment environment definition and then generating the environment.

Creating Typical custom profiles (managed nodes):

Learn how to use the **Typical** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus custom profiles. Selecting the **Typical** option creates profiles with default configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a custom profile, and have selected the **Typical** profile creation option.

About this task

In this type of configuration, the Profile Management Tool performs the following tasks:
- Assigns default values to ports, to the location of the profile, and to the names of the profile, node, and host.
- Creates a personal security certificate for the profile. The certificate has a personal key and private key, each with a default value of WebAS (you must change this password). The expiration period is one year.
- Creates a root signing security certificate for signing other certificates. The certificate has a personal key and private key, each with a default value of WebAS (you must change this password). The expiration period is 15 years.

You can choose to federate the node to an existing deployment manager during the creation process, or federate it later using the addNode command. If you decide to federate the profile during the creation process, the tool sets the Common database configuration to the same database as the deployment manager. If you decide not to federate, the database configuration is left unconfigured.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, the Federation page is displayed.

Procedure

1. In the Federation page, choose to federate the node into the deployment manager now as part of the profile creation, or at a later time and apart from profile creation.
    - If you choose to federate the node as part of the profile creation, specify the host name or IP address and SOAP port of the deployment manager, and an authentication user ID and password if administrative security is enabled on the deployment manager. Leave the **Federate this node later** check box cleared. Then click **Next**.

      The Profile Management Tool verifies that the deployment manager exists and can be contacted, and that the authentication user ID and password are valid for that deployment manager (if it is secured).

Attention: Federate the custom node during profile creation only if all the following conditions are true:

– You do not plan to use this custom node as a migration target.

– No other node is being federated. (Node federation must be serialized.)

– The deployment manager is running.

– The deployment manager is a WebSphere Process Server deployment manager. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.

– The deployment manager is at a release level the same or higher than the release level of the profile you are creating.

– The deployment manager has a JMX administrative port enabled. The default protocol is SOAP. (Click **System administration > Deployment manager > Administration services** in the administrative console of the deployment manager to verify the preferred connector type.)

If you attempt to federate a custom node when the deployment manager is not running or is not available for other reasons, a warning box prevents you from continuing. If this warning box appears, click **OK** to exit from it, and then make different selections on the Federation page.

• If you choose to federate the node at a later time and apart from profile creation, select the **Federate this node later** check box and click **Next**.

See "Federating custom nodes to a deployment manager" on page 233 for more information about how to federate a node by using the addNode command. For more information about the addNode command and its parameters, see the topic Using wsadmin scripting to run the addNode command in the WebSphere Application Server Network Deployment information center.

The Profile Summary page is displayed.

2. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:

• **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.

• **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

3. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console access the product documentation.

Results

You have created a WebSphere Process Server or WebSphere Enterprise Service Bus profile.

What to do next

If you did not federate the profile during profile creation, federate it now. The node within the profile is empty until you federate the node and use the deployment manager to customize the node.

Creating Advanced custom profiles (managed nodes):

Learn how to use the **Advanced** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus custom profiles. Selecting the **Advanced** option creates profiles with customized configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a custom profile, and have selected the **Advanced** profile creation option.

About this task

While configuring custom profiles, you can specify your own values for settings such as ports, the location of the profile, and the names for the profile, node and host. You can choose to federate the node to an existing deployment manager during the creation process, or federate it later using the addNode command.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, you are viewing the Profile Name and Location page.

Procedure
1. In the Profile Name and Location page, perform the following steps:
    a. Specify a unique name and directory path for the profile, or accept the defaults.

        Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name.

        The directory you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. The default directory is dependent on platform:

        - `Linux` `UNIX` *install_root*/profiles/*profile_name*
        - `Windows` *install_root*\profiles*profile_name*

        where *profile_name* is the name you specified. An error message is displayed if:

        - The *profile_name* you specify is not unique.
        - The directory you specify is not empty.
        - Your user ID does not have sufficient permissions for the directory.

- There is insufficient space to create the profile.

b. You can make the profile you are creating the default profile (so commands work automatically with it) by selecting the **Make this profile the default** check box. This check box appears only if you have an existing profile on your system.

   The first profile that you create on a machine is the default profile.

   The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a machine, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies. See "Profile commands in a multiprofile environment" on page 139 for more information.

   The Profile Management Tool detects ports currently used by other WebSphere products, but not the ports of other applications that might use specified ports. When federating a custom profile, the addNode command uses non-conflicting ports. This action means that you can take the default port assignments as you create the profile, and let the addNode command specify non-conflicting ports as you federate the node. Port assignments must be unique on a server. Server processes on different servers can use the same port assignments without conflict.

c. Click **Next**. (If you click **Back** and change the name of the profile, you might have to manually change the name on this page when it is displayed again.)

   The Node and Host Names page is displayed.

2. In the Node and Host Names page, specify the node and host names for the profile, or accept the defaults and click **Next**. Try to keep the node name as short as possible, but ensure that node names are unique within the deployment environment. See "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and other issues you must consider when naming.

   The Federation page is displayed.

3. In the Federation page, choose to federate the node into the deployment manager now as part of the profile creation, or at a later time and apart from profile creation.

   - If you choose to federate the node as part of the profile creation, specify the host name or IP address and SOAP port of the deployment manager, and an authentication user ID and password (if administrative security is enabled on the deployment manager). Leave the **Federate this node later** check box cleared. Then click **Next**.

     The Profile Management Tool verifies that the deployment manager exists and can be contacted, and that the authentication user ID and password are valid for that deployment manager (if it is secured).

     Important:

     Do *not* federate the custom node during profile creation if any one of the following situations is true:
     – You plan to use this custom node as a migration target.
     – Another profile is being federated. (Node federation must be serialized.)
     – The deployment manager is not running or you are not sure if it is running.

- The deployment manager has not yet been augmented into a WebSphere Process Server deployment manager.
- The deployment manager is not at a release level the same or higher than the release level of the profile you are creating.
- The deployment manager does not have a JMX administrative port enabled.
- The deployment manager is reconfigured to use the non-default remote method invocation (RMI) as the preferred Java Management Extensions (JMX) connector. (Select **System administration > Deployment manager > Administration services** in the administrative console of the deployment manager to verify the preferred connector type.)

If you attempt to federate a custom node when the deployment manager is not running or is not available for other reasons, a warning box prevents you from continuing. If this warning box appears, click **OK** to exit from it, and then make different selections on the Federation page.

- If you choose to federate the node at a later time and apart from profile creation, select the **Federate this node later** check box and click **Next**.

See "Federating custom nodes to a deployment manager" on page 233 for more information about how to federate a node by using the addNode command. For more information about the addNode command and its parameters, see the topic Using wsadmin scripting to run the addNode command in the WebSphere Application Server Network Deployment information center.

The Security Certificate (Part 1) page is displayed.

4. In the Security Certificate (Part 1) page, create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

The Security Certificate (Part 2) page is displayed.

5. Verify that the certificate information is correct, and click **Next**.

If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

When you create either or both certificates, or import either or both certificates, the keystore files that are created are:

- key.p12: Contains the default personal certificate.
- trust.p12: Contains the signer certificate from the default root certificate.
- root-key.p12: Contains the root signing certificate.

- `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
- `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
- `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify.

An imported certificate is added to the `key.p12` file or the `root-key.p12` file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

The next step depends on whether you elected to federate the profile as part of the profile creation process.

Action	Next step
Federated profile as part of profile creation	The Port Values Assignment page is displayed. Proceed to step 6.
Did not federate profile as part of profile creation	The Database Configuration page is displayed. Proceed to step 7.

6. Verify that the ports specified for the profile are unique and click **Next**.

   The Profile Management Tool detects ports currently used by other WebSphere products and displays recommended port values that do not conflict with existing ones. If you have applications other than WebSphere ones that use specified ports, verify that the ports do not conflict.

   Ports are recognized as being in use if the following conditions are satisfied:
   - The ports are assigned to a profile created under an installation performed by the current user.
   - The ports are currently in use.

   Although the tool validates ports when you access the Port Values Assignment page, port conflicts can still occur resulting from selections you make on subsequent Profile Management Tool pages. Ports are not assigned until profile creation completes.

   If you suspect a port conflict, you can investigate it after the profile is created. Determine the ports used during profile creation by examining the following file:

   - Linux   UNIX   `profile_root`/properties/portdef.props
   - Windows   `profile_root`\properties\portdef.props

   Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in an existing profile in the WebSphere Application Server Network Deployment information center. Run the `updatePorts.ant` file through the ws_ant script detailed in this topic.

   The Database Configuration page is displayed.
7. In the Database Configuration page, perform the following steps:

a. Review the database product. The database that matches the database used on the deployment manager to which this custom profile will be federated is displayed.
   b. Provide the location (directory) of the JDBC driver class path files for the database. You can accept the default values for Derby Network Server, Derby Network Server 40 or DB2 Universal Database.
   c. Click **Next**.

   The Profile Summary page is displayed.

8. In the Profile Summary page, click **Create** to create the profile, or **Back** to change the characteristics of the profile.

   When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

   Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:

   • **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.
   • **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

   The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

9. In the Profile Complete page, ensure **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to access product documentation.

Results

You have created a WebSphere Process Server or WebSphere Enterprise Service Bus profile.

What to do next

The node within the profile is empty until you federate it and use the administrative console to customize it.

In a deployment environment, you must create and configure databases, create other custom profiles and federate them to your deployment manager, create servers, create clusters if you want workload management capabilities, and perform other tasks specific to your planned installation environment. Your planned environment dictates which tasks you must perform and the order in which you perform them.

For more information about planning your installation, see the topics in the *Planning the Installation, version 7.0* PDF. To learn more about the databases required by WebSphere Process Server, see the topics under *Configuring WebSphere Process Server > Configuring databases* in the *Installing and Configuring WebSphere Process Server for Multiplatforms, version 7.0* PDF. Alternatively, view the topics in the WebSphere Process Server online information center.

Federating custom nodes to a deployment manager:

You can use the addNode command to federate a custom node into a deployment manager cell. The following instructions guide you through the process of federating and deploying custom nodes.

Before you begin

Before using this procedure, ensure that the following prerequisites are met:
- You have installed WebSphere Process Server and created a WebSphere Process Server deployment manager and a custom profile. This procedure assumes you did *not* federate the custom profile during its creation or augmentation, either with the Profile Management Tool or with the manageprofiles command-line utility.
- The deployment manager is running. If it is not, start it either by selecting **Start the deployment manager** from its First steps console or by entering the following command, where *profile_root* represents the installation location of the deployment manager profile:
  - `Linux` `UNIX` *profile_root*/bin/startManager.sh
  - `Windows` *profile_root*\bin\startManager.bat
- The deployment manager has been augmented into a WebSphere Process Server deployment manager. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.
- The deployment manager is at the same release level or higher than the custom profile you created or augmented.
- The deployment manager has a JMX administrative port enabled. The default protocol is SOAP.
- You do not plan to use this custom node as a migration target.

About this task

Federate a custom node so that it can be managed by a deployment manager. Use the addNode command to federate a custom profile into a deployment manager cell.

Procedure
1. Go to the `bin` directory of the custom profile you want to federate. Open a command window and go to one of the following directories (from a command line), depending on platform (where *profile_root* represents the installation location of the custom profile):
   - `Linux` `UNIX` *profile_root*/bin
   - `Windows` *profile_root*\bin
2. Issue the addNode command.

   Issue one of the following commands from the command line if security is not enabled:
   - `Linux` `UNIX` ./addNode.sh *deployment_manager_host deployment_manager_SOAP_port*
   - `Windows` addNode.bat *deployment_manager_host deployment_manager_SOAP_port*

Issue one of the following commands from the command line if security is enabled:

- `Linux` `UNIX` `./addNode.sh deployment_manager_host deployment_manager_SOAP_port -username userID_for_authentication -password password_for_authentication`

- `Windows` `addNode.bat deployment_manager_host deployment_manager_SOAP_port -username userID_for_authentication -password password_for_authentication`

An output window opens. If you see a message similar to the following message, your custom profile was federated successfully:

```
ADMU0003I: Node DMNDID2Node03 has been successfully federated.
```

Results

The custom profile is federated into the deployment manager. For more information about the addNode command and its parameters, see the topic Using wsadmin scripting to run the addNode command in the WebSphere Application Server Network Deployment information center.

What to do next

After federating the custom profile, go to the administrative console of the deployment manager to customize the empty node or to create a new server.

Creating Deployment environment custom profiles (managed nodes):

Learn how to use the **Deployment environment** option of the Profile Management Tool to create and configure WebSphere Process Server or WebSphere Enterprise Service Bus custom profiles. Selecting the **Deployment environment** option lets you configure a profile with customized configuration values to be used in an existing deployment environment pattern.

Before you begin

This topic assumes that you are using the Profile Management Tool to create profiles and are following the procedure in "Creating profiles using the Profile Management Tool" on page 197. As a result, it is assumed that you have started the Profile Management Tool, have chosen to create a custom profile, and have selected the **Deployment environment** profile creation option.

About this task

Select the **Deployment environment** profile creation option to set up a fully configured profile for your deployment environment. This option configures and installs all components needed for WebSphere Process Server to work. The following components are configured as part of this option:

- Business Process Choreographer
- Common Event Infrastructure
- Business Rules Manager
- Service Component Architecture

In this type of configuration, you can perform the following tasks:

- Assign customized values to ports, to the location of the profile, and to the names of the profile, node, and host.
- Specify how to federate the node to an existing deployment manager, which has a deployment environment pattern already defined.
- Specify the clusters to define on that deployment environment, as well as your own values for the Common database configuration.

As a result of following the procedure in "Creating profiles using the Profile Management Tool" on page 197, you are viewing the Profile Name and Location page.

Procedure

1. In the Profile Name and Location page, perform the following steps:

   a. Specify a unique name and directory path for the profile, or accept the defaults.

   Each profile that you create must have a name. When you have more than one profile, you can tell them apart at their highest level by this name.

   The directory you specify will contain the files that define the runtime environment, such as commands, configuration files, and log files. The default directory is dependent on the platform:

   - Linux   UNIX   `install_root/profiles/profile_name`

   - Windows   `install_root\profiles\profile_name`

   where *profile_name* is the name you specified. An error message is displayed if:

   - The *profile_name* you specify is not unique.

   - The directory you specify is not empty.

   - Your user ID does not have sufficient permissions for the directory.

   - There is insufficient space to create the profile.

   b. You can make the profile you are creating the default profile (so commands work automatically with it) by selecting the **Make this profile the default** check box. This check box appears only if you have an existing profile on your system.

   The first profile that you create on a workstation is the default profile.

   The default profile is the default target for commands that are issued from the `bin` directory in the product installation root. When only one profile exists on a workstation, every command operates on that profile. If more than one profile exists, certain commands require that you specify the profile to which the command applies. See "Profile commands in a multiprofile environment" on page 139 for more information.

   The Profile Management Tool detects ports currently used by other WebSphere products, but not ports of other applications that might use specified ports. When federating a custom profile, the addNode command uses non-conflicting ports. Because it does, you can take the default port assignments as you create the profile, and let the addNode command specify non-conflicting ports as you federate the node. Port assignments must be unique on a server. Server processes on different servers can use the same port assignments without conflict.

   c. Click **Next**. (If you click **Back** and change the name of the profile, you might have to manually change the name on this page when it is displayed again.)

   The Node and Host Names page is displayed.

2. In the Node and Host Names page, specify the node and host names for the profile, or accept the defaults and click **Next**. Try to keep the node name as short as possible, but ensure that node names are unique within the deployment environment. See "Naming considerations for profiles, nodes, servers, hosts, and cells" on page 131 for information about reserved terms and other issues you must consider when naming.

   The Federation page is displayed.

3. In the Federation page, you must federate the node into the deployment manager now as part of the profile creation. The **Federate this node later** check box does not appear on the Federation page for this type of profile creation. Specify the host name or IP address and SOAP port of the deployment manager, and an authentication user ID and password. Then click **Next**.

   To find the SOAP port number of the deployment manager, go to the *dmgr_profile_root*/logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".

   The Profile Management Tool verifies that the deployment manager exists and can be contacted, and that the authentication user ID and password are valid for that deployment manager. It also validates that there is a valid deployment environment defined on the deployment manager, and retrieves the pattern and database type back from the deployment manager.

   If you attempt to federate a custom node when the deployment manager is not running or is not available for other reasons, a warning box prevents you from continuing. If this warning box appears, correct the problem by making the necessary changes to your system and click **Next**.

   The Security Certificate (Page 1) page is displayed.

4. In the Security Certificate (Part 1) page, create a default personal certificate and a root signing certificate, or import a personal certificate and a root signing certificate from keystore files, and click **Next**.

   You can create both certificates, import both certificates, or create one certificate, and import the other certificate.

   When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the Profile Management Tool adds the signer of the personal certificate to the trust.p12 file. If you import the default personal certificate or the root signing certificate, specify the path and the password, and select the keystore type and the keystore alias for each certificate that you import.

   The Security Certificate (Part 2) page is displayed.

5. In the Security Certificate (Part 2) page, verify that the certificate information is correct, and click **Next**.

   If you create the certificates, you can use the default values or modify them to create new certificates. The default personal certificate is valid for one year by default and is signed by the root signing certificate. The root signing certificate is a self-signed certificate that is valid for 15 years by default. The default keystore password for the root signing certificate is WebAS. Change the password. The password cannot contain any double-byte character set (DBCS) characters because certain keystore types, including PKCS12, do not support these characters. The keystore types that are supported depend on the providers in the java.security file.

   When you create either or both certificates, or import either or both certificates, the keystore files that are created are:

- `key.p12`: Contains the default personal certificate.
- `trust.p12`: Contains the signer certificate from the default root certificate.
- `root-key.p12`: Contains the root signing certificate.
- `default-signers.p12`: Contains signer certificates that are added to any new keystore file that you create after the server is installed and running. By default, the default root certificate signer and a DataPower signer certificate are in this keystore file.
- `deleted.p12`: Holds certificates deleted with the deleteKeyStore task so that they can be recovered if needed.
- `ltpa.jceks`: Contains server default Lightweight Third-Party Authentication (LTPA) keys that the servers in your environment use to communicate with each other.

These files all have the same password when you create or import the certificates, which is either the default password, or a password that you specify.

An imported certificate is added to the `key.p12` file or the `root-key.p12` file.

If you import any certificates and the certificates do not contain the information that you want, click **Back** to import another certificate.

6. Verify that the ports specified for the profile are unique and click **Next**.

The Profile Management Tool detects ports currently used by other WebSphere products and displays recommended port values that do not conflict with existing ones. If you have applications other than WebSphere ones that use specified ports, verify that the ports do not conflict.

Ports are recognized as being in use if the following conditions are satisfied:
- The ports are assigned to a profile created under an installation performed by the current user.
- The ports are currently in use.

Although the tool validates ports when you access the Port Values Assignment page, port conflicts can still occur resulting from selections you make on succeeding Profile Management Tool pages. Ports are not assigned until profile creation completes.

If you suspect a port conflict, you can investigate it after the profile is created. Determine the ports used during profile creation by examining the following file:

- Linux   UNIX   *profile_root*/properties/portdef.props

- Windows   *profile_root*\properties\portdef.props

Included in this file are the keys and values used in setting the ports. If you discover port conflicts, you can reassign ports manually. To reassign ports, see the topic Updating ports in an existing profile in the WebSphere Application Server Network Deployment information center. Run the `updatePorts.ant` file through the ws_ant script detailed in this topic.

The Deployment Environment Configuration page is displayed.

7. In the Deployment Environment Configuration page, select at least one cluster to assign this node to on the deployment environment pattern and click **Next**. The page offers one to three clusters based on the deployment environment pattern defined previously on the deployment manager:

Table 50. Clusters offered per deployment environment pattern on existing deployment manager

Deployment environment pattern on deployment manager	Clusters offered
Remote messaging and remote support	• **Application deployment target**: Consists of a cluster to which user applications need to be deployed. • **Messaging infrastructure**: Consists of a cluster where messaging engines are located. • **Support infrastructure**: Consists of a cluster that hosts the Common Event Infrastructure server and other infrastructure services that are used to manage your system.
Remote messaging	• **Application deployment target**: Consists of a cluster to which user applications need to be deployed. With a remote messaging deployment environment pattern, the application deployment target cluster also assumes the functionality of the supporting infrastructure cluster. • **Messaging infrastructure**: Consists of a cluster where bus members are located.
Single cluster	• **Application deployment target**: Consists of a cluster to which user applications need to be deployed. With a single cluster deployment environment pattern, the application deployment target cluster also assumes the functionality of the messaging and the supporting infrastructure clusters.

See the following topics for more information:

- Topology types and deployment environment patterns. A deployment environment pattern specifies the constraints and requirements of the components and resources involved in a deployment environment. The patterns are designed to meet the needs of most business requirements and are intended to help you create a deployment environment in the most straightforward way.

- Functions of IBM-supplied deployment environment patterns. To design a robust deployment environment, you need to understand the functionality each cluster can provide in a particular IBM-supplied deployment environment pattern or a custom deployment environment. This knowledge can help you make the correct decisions as to which deployment environment pattern best meets your needs.

The Database Configuration page is displayed.

8. In the Database Configuration page, perform the following steps:

   a. Review the database product. The database that matches the database used on the deployment manager to which this custom profile will be federated is displayed.

      Note: Derby Network Server, DB2 for i5/OS (Toolbox), and DB2 for IBM i (Toolbox) can be accessed both locally and remotely.

    b. Provide the location (directory) of the JDBC driver class path files for the database. You can accept the default values for Derby Network Server and DB2 Universal Database.

    c. Click **Next**.

    The Profile Summary page is displayed.

9. In the Profile Summary page, click **Create** to create the profile or **Back** to change the characteristics of the profile.

   When the profile creation is complete, the Profile Complete page is displayed with the message **The Profile Management tool created the profile successfully**.

   Attention: If errors are detected during profile creation, other messages might appear in place of the success message, for example:

   • **The Profile Management tool created the profile but errors occurred**, which indicates that profile creation completed but errors were generated.

   • **The Profile Management tool cannot create the profile**, which indicates that profile creation failed completely.

   The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

10. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to access product documentation.

Results

You have created a WebSphere Process Server or WebSphere Enterprise Service Bus profile.

What to do next

Use the deployment manager to customize the node. You might add more custom nodes if not all the cluster members are assigned.

Related tasks

"Setting up deployment environments" on page 445
Setting up deployment environments involves creating the deployment environment definition and then generating the environment.

Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool:

Selected WebSphere Process Server components require a database, called the *Common* database, and a Common Event Infrastructure local database to operate. Using values you provide on the Database Configuration pages, the Profile Management Tool automatically creates the Common database and, for stand-alone server profiles, the Common Event Infrastructure database on a local system. It also creates all required tables. You must configure these databases to have a working installation.

Before you begin

This procedure assumes that you have started the Profile Management Tool and have chosen to create or augment a profile through either the Advanced or

Deployment environment profile creation or augmentation option. You are performing the procedure in one of the following topics:

- "Creating **Advanced** stand-alone server profiles" on page 202
- "Augmenting **Advanced** stand-alone server profiles" on page 307
- "Creating **Advanced** deployment manager profiles" on page 214
- "Augmenting **Advanced** deployment manager profiles" on page 315
- "Creating Deployment environment deployment manager profiles" on page 220

In the topic, you are at the step in the procedure that asks you to complete the Database Configuration page.

About this task

The following WebSphere Process Server components use the Common database:
- Application Scheduler
- Business rule group
- Mediation
- Recovery
- Relationship service
- Selector
- Event Sequencing (Lock Manager)
- Enterprise Service Bus Logger Mediation Primitive
- Messaging Engines (if you selected the **Use this database for Messaging Engines (MEs)** check box detailed in step 6 on page 243).

The Common Event Infrastructure component uses the Common Event Infrastructure database.

For more information about the various databases and database tables the WebSphere Process Server product uses, see Choosing a database.

Important: If you choose Derby Network Server or Derby Network Server 40 as your database product, ensure that the server is running on the host and port you specified during profile creation or augmentation, even if the database host is local. You can make sure that the server is running only after the profile is created or augmented.

Procedure

1. In the **Choose a database product** field, select the database product you want to use, or accept the default value of Derby Embedded or Derby Embedded 40 (for stand-alone server profiles) or Derby Network Server or Derby Network Server 40 (for deployment manager profiles).

   Restriction: Informix Dynamic Server and Microsoft SQL Server are not supported on deployment managers using the deployment environment configuration.

2. To store the database creation and configuration scripts that the profile creation or augmentation process creates in a location other than the default location, select the **Override the destination directory for generated scripts** check box and designate your new location in the **Database script output directory** field. The profile creation or augmentation process creates scripts that you or the database administrator can run manually to create new databases and their required tables, if you choose not to do so during profile creation or

augmentation. The process creates scripts for the Common database for all profile types and scripts for the Common Event Infrastructure database for stand-alone server profiles.

The default locations for the databases are as follows:

- For the Common Event Infrastructure database:

    – `Linux` `UNIX` *install_root*/profiles/*profile name*/dbscripts/ CEI_*ceiDbName*

    – `Windows` *install_root*\profiles*profile name*\dbscripts\CEI_*ceiDbName*

- For the Common database:

    – `Linux` `UNIX` *install_root*/profiles/*profile name*/dbscripts/ CommonDB/*dbType*/*dbName*

    – `Windows` *install_root*\profiles*profile name*\dbscripts\CommonDB\ *dbType**dbName*

For selected database products, you can prevent automatic creation and configuration of databases by selecting the **Delay execution of database scripts (must select if using a remote database)** check box in this page, described in step 5 on page 243.)

3. Enter your Common database name or accept the default value.

   The name of the database on IBM i using Independent Auxiliary Storage Pools (IASPs) can be the name of the IASP.

   Default Common database names differ based on the database product:

   - *SYSBAS for DB2 for i5/OS (Toolbox) and DB2 for IBM i (Toolbox)
   - WPRCSDB for all other database products

   If you plan to use an existing database, this name must match the name of that database. If you plan to create a new database and the name you specify is already associated with another WebSphere Process Server profile, you must use a different database name.

   Note: This restriction does not apply to IBM i. All profiles on IBM i use the same database name.

   Note: The Oracle database name (dbName) is the Oracle Identifier (SID) and must exist in order to create tables. When creating stand-alone server profiles, it can be shared between the Common database and the Common Event Infrastructure database. It is recommended that you remove all Oracle database resources before creating a new profile, because the Common Event Infrastructure database creates unique database resources, such as table spaces, which will fail if they exist in the Oracle server.

4. **For stand-alone server profiles only:** Enter your Common Event Infrastructure database name or accept the default value.

   Restriction: This field appears only when you are creating or augmenting a stand-alone server profile.

   The name of the database on IBM i using Independent Auxiliary Storage Pools (IASPs) can be the name of the IASP.

   Default Common Event Infrastructure database names differ based on the database product:

   - *SYSBAS for DB2, i5/OS (Toolbox), and DB2 for IBM i (Toolbox)
   - orcl for Oracle
   - EVENT for all other database products

If you plan to use an existing database, this name must match the name of that database. If you plan to create a new database and the name you specify is already associated with another WebSphere Process Server profile, you must use a different database name.

Note: This restriction does not apply to IBM i. All profiles on IBM i use the same database name.

5. Select the **Delay execution of database scripts (must select if using a remote database)** check box if you do not want to create and configure a local database automatically or create tables in an existing one during profile creation or augmentation. A local database will be created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are stored in the location specified in the **Database script output directory** field on this page.

   See the following topics for instructions on manually creating and configuring databases:

   - To create a new Common database or create tables in an existing one, see "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417.
   - **For stand-alone server profiles only:** To create a new Common Event Infrastructure database, see Manually running database configuration scripts

   Important: Do not use the Common database scripts located in the following directories (where the variable *db_type* represents the supported database product):

   - `Linux` `UNIX` *install_root*/dbscripts/CommonDB/*db_type*
   - `Windows` *install_root*\dbscripts\CommonDB*db_type*

   These default scripts have not been updated by the profile creation or augmentation process.

   Restriction: The **Delay execution of database scripts (must select if using a remote database)** option is not available for the following configurations:

   - If you chose the Derby Embedded, Derby Embedded 40, Derby Network Server, or Derby Network Server 40 product for any profile type.
   - If you chose to create a deployment manager using the Deployment environment option.

   The next step depends on whether you are creating or augmenting a stand-alone server or deployment manager profile.

Type of profile you are creating or augmenting	Next step
Stand-alone server	Proceed to step 6.
Deployment manager	Proceed to step 8 on page 244.

6. **For stand-alone server profiles only:** Select the **Use a file store for Messaging Engines (MEs)** check box to use a file store for messaging engines. If you select this check box, the messaging engines are created and configured on a file store (except for the Common Event Infrastructure messaging engine, which uses a Derby Embedded or Derby Embedded 40 local database even if this option is selected). If you do not select this check box, and do not select the **Use this database for Messaging Engines (MEs)** check box detailed in step 7 on page 244

244, the messaging engines are created and configured on the default Derby Embedded or Derby Embedded 40 database. Derby Embedded or Derby Embedded 40 databases cannot be created on remote workstations. For more information about file stores, see Administering file stores in the WebSphere Application Server Network Deployment information center.

7. **For stand-alone server profiles only:** Select the **Use this database for Messaging Engines (MEs)** check box to use the Common database for messaging engines. If you do not select this check box, and do not select the **Use a file store for Messaging Engines (MEs)** check box detailed in step 6 on page 243, the messaging engines are created and configured on the default Derby Embedded or Derby Embedded 40 database. Derby Embedded or Derby Embedded 40 databases cannot be created on remote workstations. For more information about data stores, see Administering data stores in the WebSphere Application Server Network Deployment information center.

   Restriction: This option is not available if you chose the Derby Embedded or Derby Embedded 40 product.

   Restriction: Common database cannot be used for messaging engine configuration on Informix. Do not select the **Use this database for Messaging Engines (MEs)** option for stand-alone profile creation if the Common database is Informix.

8. Click **Next**. The next step depends on the type of profile you are creating or augmenting and on the database product you chose.

Type of profile you are creating or augmenting	Next step
Stand-alone server profile with the default value of **Derby Embedded or Derby Embedded 40** selected.	The Profile Summary page is displayed. Return to step 15 on page 209 in the topic "Creating **Advanced** stand-alone server profiles" on page 202 or step 9 on page 310 in the topic "Augmenting **Advanced** stand-alone server profiles" on page 307.

Type of profile you are creating or augmenting	Next step
Stand-alone server profile with any database product other than **Derby Embedded or Derby Embedded 40** selected. Deployment manager profile with any database product selected.	The Database Configuration (Part 2) page is displayed with fields specific to the database product you selected. Review the topic "Database Configuration (Part 2) page" for information about how to complete this page. When you have completed entering information about this page, click **Next**. The tool checks that a valid connection for the Common database exists. If the database connection does not exist, you need to correct the problem either by starting up the database or altering the specified parameters before continuing. The Profile Summary page is displayed. Depending on the topic from which you accessed this one, return to one of the following steps: • Step 15 on page 209 in the topic "Creating **Advanced** stand-alone server profiles" on page 202 • Step 9 on page 310 in the topic "Augmenting **Advanced** stand-alone server profiles" on page 307 • Step 11 on page 218 in the topic "Creating **Advanced** deployment manager profiles" on page 214 • Step 5 on page 317 in the topic "Augmenting **Advanced** deployment manager profiles" on page 315 • Step 10 on page 225 in the topic "Creating Deployment environment deployment manager profiles" on page 220

Database Configuration (Part 2) page:

When you select your database product on the Database Configuration page in the Profile Management Tool, a follow-up page, called the Database Configuration (Part 2) page, asks you for database-specific information. It contains slightly different fields and default values, depending on your database product selection.

You must complete this page even if you chose to postpone creating a new database or adding tables to an existing one by selecting the **Delay execution of database scripts** check box on the previous Database Configuration page. The values you choose on the Database Configuration (Part 2) page are added to the database configuration scripts stored in the directory you specified in the **Database script output directory** field on the previous page (or in the default directory for these scripts if you did not specify a different location).

Restriction: You cannot create a new database if you are using DB2 for z/OS V8 or V9, or Oracle. In these cases, the Common database and, for a stand-alone server profile, the Common Event Infrastructure database, must exist. If you select one of these databases, a warning message alerts you to this restriction.

Choose the link for your database product from the following list to determine how to complete the Database Configuration (Part 2) page:

- "Derby Embedded or Derby Embedded 40"
- "Derby Network Server or Derby Network Server 40" on page 247
- "DB2 Universal Database" on page 247
- "DB2 Data Server" on page 248
- "DB2 for z/OS V8 and V9" on page 248
- "DB2 for i5/OS (Toolbox) and DB2 for IBM i (Toolbox)" on page 249
- "Informix Dynamic Server" on page 250
- "Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft)" on page 250
- "Oracle" on page 251

When you have completed the Database Configuration (Part 2) page, click **Next**. The tool checks that a valid connection exists to the Common database. If the tool identifies an error, you must correct the problem before continuing by either making sure that the database is up and running or altering parameters in order to make a good connection.

The Profile Summary page is displayed. Depending on the topic from which you accessed this one, return to one of the following steps:

- Step 15 on page 209 in the topic "Creating **Advanced** stand-alone server profiles" on page 202
- Step 9 on page 310 in the topic "Augmenting **Advanced** stand-alone server profiles" on page 307
- Step 11 on page 218 in the topic "Creating **Advanced** deployment manager profiles" on page 214
- Step 5 on page 317 in the topic "Augmenting **Advanced** deployment manager profiles" on page 315
- Step 10 on page 225 in the topic "Creating Deployment environment deployment manager profiles" on page 220

Derby Embedded or Derby Embedded 40

Table 51 lists the fields you must complete on the Database Configuration (Part 2) page when you select Derby Embedded or Derby Embedded 40 as your database product.

Important: If you choose Derby Embedded or Derby Embedded 40 as your database product, after profile creation or augmentation completes, ensure that the server is running on the host and port you specified during profile creation, even if the database host is local.

Table 51. Required database configuration fields for Derby Embedded or Derby Embedded 40

Field	Action needed
Schema name	Enter the database schema name. Default is APP.

Derby Network Server or Derby Network Server 40

Table 52 lists the fields you must complete on the Database Configuration (Part 2) page when you select Derby Network Server or Derby Network Server 40 as your database product.

Important: If you choose Derby Network Server or Derby Network Server 40 as your database product, after profile creation or augmentation completes, ensure that the server is running on the host and port you specified during profile creation, even if the database host is local.

Table 52. Required database configuration fields for Derby Network Server or Derby Network Server 40

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1527 or enter the correct server port number.
Schema name	Enter the database schema name. Default is APP.

DB2 Universal Database

Table 53 lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 Universal Database as your database product.

Table 53. Required database configuration fields for DB2 Universal Database

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `install_root`/universalDriver_wbi/lib on Linux and UNIX platforms, or `install_root`\universalDriver_wbi\lib on Windows platforms, or browse to the location on your system that contains the following files: • `db2jcc.jar` • `db2jcc_license_cu.jar` *or* `db2jcc_license_cisuz.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.

Table 53. Required database configuration fields for DB2 Universal Database (continued)

Field	Action needed
Server port	Accept the default value of 50000 or enter the correct server port number.
Schema name	Enter the database schema name. Default is `WPRCDB`.

DB2 Data Server

Table 54 lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 Data Server as your database product.

Table 54. Required database configuration fields for DB2 Data Server

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `install_root`/universalDriver_wbi/lib on Linux and UNIX platforms, or `install_root`\universalDriver_wbi\lib on Windows platforms, or browse to the location on your system that contains the following files: • `db2jcc.jar` • `db2jcc_license_cu.jar` *or* `db2jcc_license_cisuz.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 50000 or enter the correct server port number.
Schema name	Enter the database schema name. Default is `WPRCDB`.

DB2 for z/OS V8 and V9

Table 55 lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 for z/OS V8 and V9 as your database product. You cannot create a new database using these databases. The Common database and, for a stand-alone server profile, the Common Event Infrastructure database, must exist.

Table 55. Required database configuration fields for DB2 for z/OS V8 and V9

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.

Table 55. Required database configuration fields for DB2 for z/OS V8 and V9 (continued)

Field	Action needed
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • `db2jcc.jar` • `db2jcc_license_cisuz.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Enter the database server host name.
Server port	Accept the default value of 446 or enter the correct server port number.
Database alias name	Enter the database alias name.
Connection location	Enter the connection location.
Storage group name	Enter the storage group name.

DB2 for i5/OS (Toolbox) and DB2 for IBM i (Toolbox)

Table 56 lists the fields you must complete on the Database Configuration (Part 2) page when you select or DB2 for IBM i (Toolbox) as your database product. This selection is also valid for DB2 for i5/OS (Toolbox).

Table 56. Required database configuration fields for DB2 for IBM i (Toolbox) or DB2 for IBM i (Toolbox)

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `/QIBM/ProdData/HTTP/Public/jt400/lib` or browse to the location on your system that contains the following file: • `jt400.jar` An error message is displayed if the file cannot be found at the specified location.
Database server host name (for example IP address)	Enter the database server host name.
Database collection name	Accept the default value of `WPRCSDB` or enter the correct schema name. To prevent naming conflicts within the specified database, specify a schema name whose first three characters are unique from the names of other schemas residing in the database.

Informix Dynamic Server

Table 57 lists the fields you must complete on the Database Configuration (Part 2) page when you select Informix Dynamic Server as your database product.

Table 57. Required database configuration fields for Informix Dynamic Server

Field	Action needed
Directory of database server installation	Indicates the database installation directory if you are using Informix databases.
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • `ifxjdbc.jar` • `ifxjdbcx.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1526 or enter the correct server port number.
Instance name	Enter the correct instance name.

Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft)

Table 58 lists the fields you must complete on the Database Configuration (Part 2) page when you select Microsoft SQL Server (DataDirect) or Microsoft SQL Server (Microsoft) as your database product.

Table 58. Required database configuration fields for Microsoft SQL Server DataDirect and Microsoft SQL Server (Microsoft)

Field	Action needed
CEI database user name	Enter the CEI database user name.
CEI database password	Enter a password to authenticate with the CEI database.
Confirm password	Confirm the password.
Common database user name	Enter the user name to authenticate with the database.
Common database password	Enter a password to authenticate with the database.
Confirm password	Confirm the password.

Table 58. Required database configuration fields for Microsoft SQL Server DataDirect and Microsoft SQL Server (Microsoft) (continued)

Field	Action needed
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • `sqlserver.jar` • `base.jar` • `util.jar` Also, the file `spy.jar` must be available in the following location relative to the location of the JDBC driver class path files: • `Linux` `UNIX` `../spy/spy.jar` • `Windows` `..\spy\spy.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Database server name	Enter the database server name.
Server port	Accept the default value of 1433 or enter the correct server port number.
Admin user name	Enter the user ID that has privileges to create and drop databases and users or accept the default value of `sa`. This ID is required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Password	Enter the password for the user **Admin user name** ID.
Confirm password	Confirm the password.

Oracle

Table 59 lists the fields you must complete on the Database Configuration (Part 2) page when you select Oracle as your database product. You cannot create a new database using this database.

Important: You must have a user ID that has SYSDBA privileges before creating any profile.

Table 59. Required database configuration fields for Oracle

Field	Action needed
Directory of database server installation	Enter or browse for the database server installation. Required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Business Space database user name	User ID for the Business Space database. This option only appears if BSpace is enabled.
Business Space database password	Enter a password to authenticate with the Business Space database.
Confirm password	Confirm the password.

Table 59. Required database configuration fields for Oracle (continued)

Field	Action needed
CEI database user name	User ID for the Common Event Infrastructure database.
CEI database password	Enter a password to authenticate with the Common Event Infrastructure database.
Confirm password	Confirm the password.
Common database user name	User ID for the Common database.
Password	Enter a password to authenticate with the Common database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the file `ojdbc6.jar`. You must install the `ojdbc6.jar` driver to access the Oracle database. **Important:** Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle Web site. An error message is displayed if the files cannot be found at the specified location.
JDBC driver type	Click **OCI** or **Thin**.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1521 or enter the correct server port number.
System administrator user name	Enter the user ID that has privileges to create and drop databases and users or accept the default value of SYSUSER. Required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Password	Enter the password for the user **Admin user name** ID.
Confirm password	Confirm the password.

If you selected **Use this database for Messaging Engines (MEs)** in the first Database Configuration screen, the Database Configuration (Part 3) page is displayed. Table 60 lists the fields you must complete.

Table 60. Required database configuration fields for using Oracle with Messaging Engines

Field	Action needed
Business Process Choreographer messaging engine	
User name	Enter the Business Process Choreographer messaging engine user ID. This option only appears if BPC is enabled.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
CEI bus messaging engine	
User name	Enter the CEI bus messaging engine user ID.

Table 60. Required database configuration fields for using Oracle with Messaging Engines (continued)

Field	Action needed
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
SCA application bus messaging engine	
User name	Enter the SCA application bus messaging engine user ID.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
SCA system bus messaging engine	
User name	Enter the SCA system bus messaging engine user ID.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.

Creating profiles using the manageprofiles command-line utility

Learn about creating a profile from the command line using the manageprofiles command-line utility and a property file.

Before you begin

To find out more about the manageprofiles command-line utility, see "manageprofiles command-line utility" on page 375.

Before you run the manageprofiles command-line utility ensure that you have completed the following tasks:

- You have reviewed the full list of prerequisites for creating or augmenting a profile at "Prerequisites for creating or augmenting profiles" on page 189.
- You have reviewed example profile creation commands in "Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 255 or "Example: Creating profiles with manageprofiles command-line utility and Oracle database" on page 268.
- You have verified that you are not already running the manageprofiles command-line utility on the same profile. If an error message is displayed, determine if there is another profile creation or augmentation action in progress. If so, wait until it completes.

Security role required for this task: See "Granting write permission of files and directories to nonroot users for profile creation" on page 193.

Note: On i5/OS platforms: You must have operating system permissions to read, write, and run commands in the *user_data_root*/profiles directory.

To use the manageprofiles command-line utility to create a profile, perform the following steps.

Procedure

1. Determine the kind of profile you want to create, which in turn determines the template to use for your new profile (using the **-templatePath** option). The following templates are available:

- `default.wbiserver`: for a WebSphere Process Server stand-alone server profile, which defines a stand-alone server.
- `dmgr.wbiserver`: for a WebSphere Process Server deployment manager profile, which defines a deployment manager. A *deployment manager* provides one administrative interface to a logical group of servers on one or more workstations.
- `managed.wbiserver`: for a WebSphere Process Server custom profile, which, when federated to a deployment manager, defines a managed node. If you have decided that your solution requires a deployment environment, your runtime environment requires one or more managed nodes. A *custom profile* contains an empty node that you must federate into a deployment manager cell to make operational. Federating the custom profile changes it into a managed node. Do not federate a node unless the deployment manager you are federating to is at a release level the same or higher than that of the custom profile you are creating. Also, WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.
- `default.esbserver`: for a WebSphere Enterprise Service Bus stand-alone server profile, which defines a stand-alone server.
- `dmgr.esbserver`: for a WebSphere Enterprise Service Bus deployment manager profile, which defines a deployment manager.
- `managed.esbserver`: for a WebSphere Enterprise Service Bus custom profile, which, when federated to a deployment manager, defines a managed node. Do not federate a node unless the deployment manager you are federating to is at a release level the same or higher than that of the custom profile you are creating. WebSphere Enterprise Service Bus profiles can use a WebSphere Enterprise Service Bus or WebSphere Process Server deployment manager.

Templates for each profile are located in the *install_root*/`profileTemplates` directory.

2. Determine which parameters are required for your type of profile by reviewing the example profile creation commands in "Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 255 or "Example: Creating profiles with manageprofiles command-line utility and Oracle database" on page 268.

3. Determine the values that you want to supply for the profile by reviewing the default values in the "manageprofiles parameters" on page 377 topic to see if they are what you need for your profile.

   Note: If you create profiles in WebSphere Process Server using the manageprofiles command-line utility without specifying the `samplesPassword` parameter, the `INSTCONFPARTIALSUCCESS` message is returned. This occurs when the following criteria are met:
   - You installed the samples during WebSphere Process Server or WebSphere Application Server installation.
   - You use the manageprofiles command-line utility to create the profiles.
   - The `samplesPassword` parameter is not specified in the manageprofiles command-line utility.

4. Run the file from the command line. Here are some simple examples. For more complex examples, see "Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 255 or "Example: Creating profiles with manageprofiles command-line utility and Oracle database" on page 268.

- **On i5/OS platforms:**`manageprofiles -create -templatePath`
  `install_root/profileTemplates/default.wbiserver`

- `Linux` `UNIX` `manageprofiles.sh -create -templatePath`
  `install_root/profileTemplates/default.wbiserver`

- `Windows` `manageprofiles.bat -create -templatePath` `install_root\`
  `profileTemplates\default.wbiserver`

If you have created a response file, use the **-response** parameter: `-response`
`myResponseFile`

The following example shows a response file for a create operation:

```
create
profileName=testResponseFileCreate
profilePath=profile_root
templatePath=install_root/profileTemplates/default.wbiserver
nodeName=myNodeName
cellName=myCellName
hostName=myHostName
omitAction=myOptionalAction1, myOptionalAction2
```

The command displays status as it runs. Wait for it to finish. Normal syntax checking on the response file applies as the file is parsed like any other response file. Individual values in the response file are treated as command-line parameters.

What to do next

You can see that your profile creation completed successfully if you receive a `INSTCONFSUCCESS: Profile creation succeeded.` message, and you can check the following log file:

- **On i5/OS platforms:** *user_data_root*/profileRegistry/logs/manageprofiles/
  *profile_name*_create.log

- `Linux` `UNIX` *install_root*/logs/manageprofiles/
  *profile_name*_create.log

- `Windows` *install_root*\logs\manageprofiles*profile_name*_create.log

Run the Installation Verification Test (IVT) tool to verify that the profile was created successfully. To do this, run the following command:

- **On i5/OS platforms:** *profile_root*/bin/wbi_ivt

- `Linux` `UNIX` **On Linux and UNIX platforms:** *profile_root*/bin/
  wbi_ivt.sh

- `Windows` **On Windows platforms:** *profile_root*\bin\wbi_ivt.bat

Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples:

Example profile creation commands to help you create stand-alone server, deployment manager, and custom profiles using the manageprofiles command-line utility on your installation.

Stand-alone server profile

The following command example creates a WebSphere Process Server stand-alone server profile called *my_WPSSA_profile* on a Windows server. The parameters in Table 61 on page 256 and Table 62 on page 257 specify the following:

- The DB2 Universal database product will be used for both the Common and Common Event Infrastructure databases, which are both assumed to already exist on the localhost. Both databases are set to be configured later (the **-dbDelayConfig "false"** and **-dbDelayConfig "true"** command parameter values specify that configuration scripts be created but not run). For complete listings of database-related manageprofiles parameters, see the topics "manageprofiles parameters for Common database configuration (per database product)" on page 280 and "manageprofiles parameters for Common Event Infrastructure database configuration (per database product)" on page 291.
- The Windows service will be set for manual startup.
- A sample Business Process Choreographer implementation will *not* be created.
- The Business Rules Manager will be configured.
- Business Space powered by WebSphere will *not* be configured.
- The profile creation process will set the port values automatically (except for database-related ports). The process will validate the new profile against other profiles to ensure there are no port conflicts.

  Tip: To override the port values that the manageprofiles command-line utility will specify, use the **-portsFile** parameter. See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.
- Administrative security will be enabled.

Table 61 shows manageprofiles command-line utility parameters with example values used to create a stand-alone server profile.

Table 61. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ default.wbiserver" (must be fully qualified)
-profileName	"*my_WPSSA_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-dbServerPort	"50000"
-ceiDbName	"event"
-dbDelayConfig	"false"
-dbHostName	"localhost"
-ceiDbAlreadyConfigured	"false"
-configureBPC	"false"
-dbType	"DB2_Universal" or "DB2_DataServer"
-dbName	"WPRCSDB"
-dbCreateNew	"false"
-dbDelayConfig	"true"
-dbUserId	"*db_id*"
-dbPassword	"*db_pwd*"
-dbDriverType	"4"
-dbHostName	"localhost"

Parameter	Value
-dbServerPort	"50000"
-dbCommonForME	"false"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-configureBSpace	"false"
-configureBRM	"true"

Table 62 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 62. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles*my_WPSSA_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*Node*node_number*"
-cellName	"*host_name*Node*node_number*cell_number*Cell"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbOutputscriptDir	"*install_root*\profiles*my_WPSSA_profile*\dbscripts\CEI_event"
-dbJDBCClasspath	"*install_root*\universalDriver_wbi\lib"
-dbJDBCClasspath	"*install_root*\universalDriver_wbi\lib"
-dbOutputScriptDir	"*install_root*\profiles*my_WPSSA_profile*\dbscripts\CommonDB\DB2\WPRCSDB"

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus stand-alone server profile called *my_WESBSA_profile*. There is a difference:
• The Derby Embedded or Derby Embedded 40 database product will be used for both the Common and Common Event Infrastructure databases, which are set to be created and configured on the localhost during the profile creation process.

Table 63 shows manageprofiles command-line utility parameters with example values.

Table 63. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\default.esbserver" (must be fully qualified)
-profileName	"*my_WESBSA_profile*"

Table 63. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ceiDbName	"event"
-dbDelayConfig	"true"
-ceiDbAlreadyConfigured	"false"
-dbType	"DERBY_EMBEDDED" "DERBY_EMBEDDED40"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbDelayConfig	"false"
-dbCommonForME	"false"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-configureBSpace	"false"

Table 64 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 64. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles*my_WESBSA_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*Node*node_number*"
-cellName	"*host_name*Node*node_number*cell_number*Cell"
Windows -winserviceStartupType	"manual"
Windows -winserviceCheck	"true"
Windows -winserviceAccountType	"localsystem"
Windows -winserviceUserName	"Administrator"
-dbOutputScriptDir	"*install_root*\profiles*my_WESBSA_profile*\dbscripts\CommonDB\Derby\WPRCSDB"

Deployment manager profile (without deployment environment setup)

The following command example creates a deployment manager profile called *my_WPSDMGR_profile* on a Windows server.

The parameters in Table 65 on page 259 and Table 66 on page 259 specify the following:
- The DB2 Universal database product will be used for the Common database, which is assumed to exist on a remote host. The database is set to be configured later (the **-dbDelayConfig "true"** command parameter value specifies that configuration scripts be created but not run). For a complete listing of

database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.

- The Windows service will be set for manual startup.
- The profile creation process will set the port values automatically (except for database-related ports). The process will validate the new profile against other profiles to ensure there are no port conflicts.

  Tip: To override the port values that the manageprofiles command-line utility will specify, use the **-portsFile** parameter. See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.
- Administrative security will be enabled.

Table 65 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 65. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\dmgr.wbiserver" (must be fully qualified)
-profileName	"*my_WPSDMGR_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"DB2_Universal" or "DB2_DataServer"
-dbName	"WPRCSDB"
-dbCreateNew	"false"
-dbDelayConfig	"true"
-dbUserId	"*db_id*"
-dbPassword	"*db_pwd*"
-dbDriverType	"4"
-dbHostName	"*remote_host_name*"
-dbServerPort	"50000"

Table 66 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 66. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles*my_WPSDMGR_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
`Windows` -winserviceCheck	"true"

Table 66. Defaulted manageprofiles command-line utility parameters (continued)

Parameter	Default values
Windows -winserviceAccountType	"localsystem"
Windows -winserviceStartupType	"manual"
Windows -winserviceUserName	"Administrator"
-dbJDBCClasspath	"*install_root*\universalDriver_wbi\lib"
-dbOutputScriptDir	"*install_root*\profiles*my_WPSDMGR_profile*\ dbscripts\CommonDB\DB2\WPRCSDB"

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus deployment manager profile called *my_WESBDMGR_profile*. The difference is the Derby Network Server or Derby Network Server 40 database product will be used for the Common database, which is set to be created and configured on the localhost during the profile creation process.

Table 67 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 67. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.esbserver" (must be fully qualified)
-profileName	"*my_WESBDMGR_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbDelayConfig	"false"
-dbUserId	"*db_id*"
-dbPassword	"*db_pwd*"
-dbHostName	"localhost"
-dbServerPort	"1528"

Table 68 on page 261 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 68. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WESBDMGR_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbOutputScriptDir	"*install_root*\profiles\ *my_WESBDMGR_profile*\dbscripts\ CommonDB\Derby\WPRCSDB"

Custom profile (without deployment environment setup)

The following command example creates a custom profile called *my_WPSCUSTOM_profile* on a Windows server.

This example is set to operate with the deployment manager profile created above.

The parameters in Table 69 and Table 70 on page 262 specify the following:
- The DB2 Universal database product will be used for the Common database, which is assumed to already exist. The custom profile creation needs to point to the database used by the deployment manager to which the custom profile will be federated.
- Administrative security will be enabled on the deployment manager to which the custom profile will be federated.

See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.

Table 69 shows manageprofiles command-line utility parameters with example values used to create a custom profile.

Table 69. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ managed.wbiserver" (must be fully qualified)
-profileName	"*my_WPSCUSTOM_profile*"
-dmgrHost	"*remote_host*"

Table 69. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-dmgrPort	"8882" (To find the -dmgrPort value, go to the *dmgr_profile_root*\logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".)
-dmgrAdminPassword	"*admin_pwd*"
-dmgrAdminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"DB2_Universal" or "DB2_DataServer"
-dbJDBCClasspath	"*install_root*\universalDriver_wbi\lib"

Table 70 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 70. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles*my_WPSCUSTOM_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*Node*node_number*"

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus custom profile called *my_WESBCUSTOM_profile*. The difference is the Derby Network Server or Derby Network Server 40 database product will be used for the Common database on the deployment manager to which the custom profile will be federated. This example is set to operate with the WebSphere Enterprise Service Bus deployment manager profile created above.

Table 71 shows manageprofiles command-line utility parameters with example values used to create a custom profile.

Table 71. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\managed.esbserver" (must be fully qualified)
-profileName	"*my_WESBCUSTOM_profile*"
-dmgrHost	"*remote_host*"

Table 71. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-dmgrPort	"8885" (To find the -dmgrPort value, go to the *dmgr_profile_root*\logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".)
-dmgrAdminPassword	"*admin_pwd*"
-dmgrAdminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbJDBCClasspath	"*install_root*\derby\lib"

Table 72 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 72. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WESBCUSTOM_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*Node*node_number*"

Deployment manager profile (with deployment environment setup)

The following command example creates a deployment manager profile called *my_WPSDMGR_DE_profile* on a Windows server.

The parameters in Table 73 on page 264 and Table 74 on page 264 specify the following:
- The profile creation process will automatically configure a deployment environment (specified by the parameters **-ndtopology "true"** and **-topologyPattern "Reference"**).
- The Derby Network Server or Derby Network Server 40 database product will be used for the Common database, which is set to be created and configured on the localhost during the profile creation process. For a complete listing of database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.
- The Windows service will be set for manual startup.
- The profile creation process will set the port values automatically (except for database-related ports). The process will validate the new profile against other profiles to ensure there are no port conflicts.

  Tip: To override the port values that the manageprofiles command-line utility will specify, use the **-portsFile** parameter. See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.

- Administrative security will be enabled.

Table 73 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 73. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.wbiserver" (must be fully qualified)
-profileName	"*my_WPSDMGR_DE_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"true"
-topologyPattern	"Reference"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbDelayConfig	"false"
-dbUserId	"*db_id*"
-dbPassword	"*db_pwd*"
-dbHostName	"localhost"
-dbServerPort	"1529"

Table 74 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 74. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WPSDMGR_DE_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbOutputScriptDir	"*install_root*\profiles\ *my_WPSDMGR_DE_profile*\dbscripts\ CommonDB\Derby\WPRCSDB"

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus deployment manager profile called *my_WESBDMGR_DE_profile*.

Table 75 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 75. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.esbserver" (must be fully qualified)
-profileName	"*my_WESBDMGR_DE_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"true"
-topologyPattern	"Reference"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbDelayConfig	"false"
-dbUserId	"*db_id*"
-dbPassword	"*db_pwd*"
-dbHostName	"localhost"
-dbServerPort	"1530"

Table 76 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 76. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WESBDMGR_DE_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbOutputScriptDir	"*install_root*\profiles\ *my_WESBDMGR_DE_profile*\dbscripts\ CommonDB\Derby\WPRCSDB"

Custom profile (with deployment environment setup)

The following command example creates a custom profile called *my_WPSCUSTOM_DE_profile* on a Windows server. This example is set to operate with the deployment manager profile *for a deployment environment* created above.

The parameters in Table 77 and Table 78 on page 267 specify the following:
- The profile creation process will automatically assign the profile to a deployment environment (specified by the parameters **-ndtopology "true"** and **-topologyRole ADT Messaging Support**).
- The Derby Network Server or Derby Network Server 40 database product will be used for the Common database, which is assumed to already exist. The custom profile creation needs to point to the database used by the deployment manager to which the custom profile will be federated. For a complete listing of database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.
- Administrative security will be enabled on the deployment manager to which the custom profile will be federated.

See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.

Table 77 shows manageprofiles command-line utility parameters with example values used to create a custom profile.

Table 77. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ managed.wbiserver" (must be fully qualified)
-profileName	"*my_WPSCUSTOM__DE_profile*"
-dmgrHost	"*remote_host*"
-dmgrPort	"8890" (To find the -dmgrPort value, go to the *dmgr_profile_root*\logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".)
-dmgrAdminPassword	"*admin_pwd*"
-dmgrAdminUserName	"*admin_id*"
-ndtopology	"true"
-topologyRole	"ADT Support Messaging"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbJDBCClasspath	"*install_root*\derby\lib"

Table 78 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 78. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WPSCUSTOM_DE_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*Node*node_number*"

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus custom profile called *my_WESBCUSTOM_DE_profile*. This example is set to operate with the WebSphere Enterprise Service Bus deployment manager profile *for a deployment environment* created above.

Table 79 shows manageprofiles command-line utility parameters with example values used to create a custom profile.

Table 79. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ managed.esbserver" (must be fully qualified)
-profileName	"*my_WESBCUSTOM__DE_profile*"
-dmgrHost	"*remote_host*"
-dmgrPort	"8897" (To find the -dmgrPort value, go to the *dmgr_profile_root*\logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".)
-dmgrAdminPassword	"*admin_pwd*"
-dmgrAdminUserName	"*admin_id*"
-ndtopology	"true"
-topologyRole	"ADT Support Messaging"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbJDBCClasspath	"*install_root*\derby\lib"

Table 80 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 80. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WESBCUSTOM_DE_profile*"
-hostName	"*host_name*"

Table 80. Defaulted manageprofiles command-line utility parameters (continued)

Parameter	Default values
-nodeName	"*host_name*Node*node_number*"

Example: Creating profiles with manageprofiles command-line utility and Oracle database:

Example profile creation commands to help you create stand-alone server and deployment manager profiles using the manageprofiles command-line utility on your installation with an Oracle database.

Stand-alone server profile

The following command example creates a WebSphere Process Server stand-alone server profile called *my_WPSSA_profile* on a Windows server.

The parameters in Table 81 on page 269, Table 82 on page 269, and Table 83 on page 270 specify the following features:

- The Oracle database product will be used for both the Common and Common Event Infrastructure databases, which are both assumed to already exist on the localhost. Both databases are set to be configured later (the **-dbDelayConfig "true"** command parameter value specifies that configuration scripts be created but not run). For complete listings of database-related manageprofiles parameters, see the topics "manageprofiles parameters for Common database configuration (per database product)" on page 280 and "manageprofiles parameters for Common Event Infrastructure database configuration (per database product)" on page 291.
- The Windows service will be set for manual startup.
- A sample Business Process Choreographer configuration will be created.
- The Business Rules Manager will *not* be configured.
- Business Space powered by WebSphere will be configured.
- The profile creation process will set the port values automatically (except for database-related ports). The process will validate the new profile against other profiles to ensure there are no port conflicts.

  Tip: To override the port values that the manageprofiles command-line utility will specify, use the **-portsFile** parameter. See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.
- Administrative security will be enabled.

There are two configuration options available:

- Optional: If you want all of the schema user IDs and tables to be created as part of the profile creation, you must provide a user ID that has SYSDBA privileges in the Oracle database. This ID is used to create the schemas and tables, but is not persisted anywhere in the configuration.
- Optional: If you do not want to provide the SYSDBA user ID, you can export the scripts and execute them manually.

  For both of these options, you can select a specific schema user ID for each of the components.

Table 81 on page 269 shows manageprofiles command-line utility parameters with example values used to create a stand-alone server profile.

Table 81. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ default.wbiserver" (must be fully qualified)
-profileName	"*my_WPSSA_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-configureBPC	"true"
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-ceiDbName	"EVENT"
-dbDelayConfig	"true"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-dbCommonForME	"true"
-dbPassword	"*db_pwd*"
-dbDriverType	"oracle_thin"
-dbJDBCClasspath	"oracle_library_directory"
-dbServerPort	"1521"
-configureBSpace	"true"
-configureBRM	"false"

Table 82 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 82. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles*my_WPSSA_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*Node*node_number*"
-cellName	"*host_name*Node*node_number*cell_number*Cell"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbOutputscriptDir	"*install_root*\profiles*my_WPSSA_profile*\ dbscripts\"
-dbHostName	"local_host_name"

Table 83 shows additional manageprofiles command-line utility parameters that are not displayed via the Profile Management Tool that can be specified to select your own user name and password combinations for Oracle.

Table 83. Additional manageprofiles command-line utility parameters for Oracle

Parameter	Value	Remarks
-dbSysUserId	"*sys_user_id*"	This ID must have SYSDBA privileges. Do not use the Oracle internal user 'sys'. This parameter is needed if you want to configure the database and its objects during profile creation [when dbDelayConfig = "FALSE"]
-dbSysPassword	"*sys_pwd*"	This parameter is needed if you want to configure the database and its objects during profile creation [when dbDelayConfig = "FALSE"]
-dbCommonUserId	"*common_db_userID*" (used to create Common DB objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCommonUserId is ORCCOMM
-dbCommonPassword	"*common_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCommonPassword will be set to dbPassword. For example: dbCommonPassword = dbPassword
-dbBSpaceUserId	"*bspace_db_userID*" (used to configure Business Space)	This parameter is needed if you require your own Business Space schema. If not, the default value (IBMBUSSP) will be set.
-dbBSpacePassword	"*bspace_db_pwd*" (used to configure Business Space)	This parameter is needed if you need your own Business Space password otherwise default value will be set in the following order: dbBSpacePassword = "YouNameIt" else dbBSpacePassword = dbPassword [if exists] else dbBSpacePassword = IBMBUSSP
-dbCeiUserId	"*cei_userID*" (used to create CEI objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiUserId is ORCCEID
-dbCeiPassword	"*cei_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example, dbCeiPassword = dbPassword
	All the parameters below are only valid if -dbCommonForME = "true"	

Table 83. Additional manageprofiles command-line utility parameters for Oracle (continued)

Parameter	Value	Remarks
-dbBPCMeUserId	"*bpc_me_userID*" (used to create BPC ME objects) (only valid if -configureBPC = "true")	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbBPCMeUserId is ORCBM00
-dbBPCMePassword	"*bpc_me_pwd*" (only valid if -configureBPC = "true")	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example, dbBPCMePassword = dbPassword
-dbCeiMeUserId	"*cei_me_userID*" (used to create CEI ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiMeId is ORCCM00
-dbCeiMePassword	"*cei_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbCeiMePassword = dbPassword
-dbAppMeUserId	"*app_me_userID*" (used to create SCAAPP ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbAppMeId is ORCSA00
-dbAppMePassword	"*app_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword
-dbSysMeUserId	"*sys_me_userID*" (used to create SCASYS ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbSysMeUserId is ORCSS00
-dbSysMePassword	"*sys_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus stand-alone server profile called *my_WESBSA_profile*. The difference is the database is set to be configured now (the -dbDelayConfig "false" command parameter value specifies that configuration scripts be run).

Table 84 shows manageprofiles command-line utility parameters with example values.

Table 84. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ default.esbserver" (must be fully qualified)
-profileName	"*my_WESBSA_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-dbType	"ORACLE"
-dbUserId	"*cei_id*"
-dbUserId	"*cei_pwd*"
-dbName	"WPRCSDB"
-ceiDbName	"EVENT"
-dbDelayConfig	"false"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-dbCommonForME	"true"
-dbLocation	"*oracle_install_directory*"
-dbPassword	"*db_pwd*"
-dbDriverType	"oracle_thin"
-dbJDBCClasspath	"oracle_library_directory"
-dbServerPort	"1521"
-dbSysUserId	"*sys_user_id*"
-dbSysPassword	"*sys_pwd*"
-configureBSpace	"true"

Table 85 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 85. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles*my_WESBSA_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*Node*node_number*"
-cellName	"*host_name*Node*node_number*cell_number*Cell"

Parameter	Default values
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceUserName	"Administrator"
-dbOutputScriptDir	"*install_root*\profiles*my_WESBSA_profile*\ dbscripts\"
-dbHostName	"*local_host_name*"

Table 86 shows additional manageprofiles command-line utility parameters that are not displayed via the Profile Management Tool that can be specified to select your own user name and password combinations for Oracle.

Table 86. Additional manageprofiles command-line utility parameters for Oracle

Parameter	Default values	Remarks
-dbCommonUserId	"*common_db_userID*" (used to create Common DB objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCommonUserId is ORCCOMM
-dbCommonPassword	"*common_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCommonPassword will be set to dbPassword. For example: dbCommonPassword = dbPassword
-dbBSpaceUserId	"*bspace_db_userID*" (used to configure Business Space)	This parameter is needed if you require your own Business Space schema. If not, the default value (IBMBUSSP) will be set.
-dbBSpacePassword	"*bspace_db_pwd*" (used to configure Business Space)	This parameter is needed if you need your own Business Space password otherwise default value will be set in the following order: dbBSpacePassword = "YouNameIt" else dbBSpacePassword = dbPassword [if exists] else dbBSpacePassword = IBMBUSSP
-dbCeiUserId	"*cei_userID*" (used to create CEI objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiUserId is ORCCEID

Table 86. Additional manageprofiles command-line utility parameters for Oracle (continued)

Parameter	Default values	Remarks
-dbCeiPassword	"*cei_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example, dbCeiPassword = dbPassword
	All the parameters below are only valid if -dbCommonForME = "true"	
-dbCeiMeUserId	"*cei_me_userID*" (used to create CEI ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiMeId is ORCCM00
-dbCeiMePassword	"*cei_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbCeiMePassword = dbPassword
-dbAppMeUserId	"*app_me_userID*" (used to create SCAAPP ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbAppMeId is ORCSA00
-dbAppMePassword	"*app_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword
-dbSysMeUserId	"*sys_me_userID*" (used to create SCASYS ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbSysMeUserId is ORCSS00

Parameter	Default values	Remarks
-dbSysMePassword	"*sys_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword

Deployment manager profile (without deployment environment setup)

The following command example creates a deployment manager profile called *my_WPSDMGR_profile* on a Windows server.

The parameters in Table 87 and Table 88 on page 276 specify the following:

- The Oracle database product will be used for the Common database, which is assumed to exist on a remote host. The database is set to be configured later (the **-dbDelayConfig "true"** command parameter value specifies that configuration scripts be created but not run). For a complete listing of database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.
- The Windows service will be set for manual startup.
- The profile creation process will set the port values automatically (except for database-related ports). The process will validate the new profile against other profiles to ensure there are no port conflicts.

  Tip: To override the port values that the manageprofiles command-line utility will specify, use the **-portsFile** parameter. See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.
- Administrative security will be enabled.

Table 87 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 87. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.wbiserver" (must be fully qualified)
-profileName	"*my_WPSDMGR_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-dbDelayConfig	"true"
-dbPassword	"*db_pwd*"

Table 87. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-dbDriverType	"oracle_thin"
-dbHostName	"*remote_host_name*"
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"

Table 88 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 88. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles*my_WPSDMGR_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbOutputScriptDir	"*install_root*\profiles*my_WPSDMGR_profile*\dbscripts\"

Table 89 shows additional manageprofiles command-line utility parameters that are not displayed via the Profile Management Tool that can be specified to select your own user name and password combinations for Oracle.

Table 89. Additional manageprofiles command-line utility parameters for Oracle

Parameter	Default values
-dbSysUserId	"*sys_userID*" (used to create SCASYS ME objects)
-dbSysPassword	"*sys_pwd*"
-dbCommonUserId	"*common_db_userID*" (used to create Common DB objects)
-dbCommonPassword	"*common_db_pwd*"

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus deployment manager profile called *my_WESBDMGR_profile*. The difference is the database is set to be configured now (the **-dbDelayConfig "false"** command parameter value specifies that configuration scripts be run).

Table 90 on page 277 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 90. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.esbserver" (must be fully qualified)
-profileName	"*my_WESBDMGR_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-dbDelayConfig	"false"
-dbLocation	"*oracle_install_directory*"
-dbPassword	"*db_pwd*"
-dbDriverType	"oracle_thin"
-dbHostName	"localhost"
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"
-dbSysUserId	"*sys_user_id*"
-dbSysPassword	"*sys_pwd*"

Table 91 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 91. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WESBDMGR_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbOutputScriptDir	"*install_root*\profiles\ *my_WESBDMGR_profile*\dbscripts\"

Table 92 on page 278 shows additional manageprofiles command-line utility parameters that are not displayed via the Profile Management Tool that can be specified to select your own user name and password combinations for Oracle.

Table 92. Additional manageprofiles command-line utility parameters for Oracle

Parameter	Default values
-dbCommonUserId	"*common_db_userID*" (used to create Common DB objects)
-dbCommonPassword	"*common_db_pwd*"

Deployment manager profile (with deployment environment setup)

The following command example creates a deployment manager profile called *my_WPSDMGR_DE_profile* on a Windows server.

The parameters in Table 93 and Table 94 on page 279 specify the following:
- The profile creation process will automatically configure a deployment environment (specified by the parameters **-ndtopology "true"** and **-topologyPattern "Reference"**).
- The Oracle database product will be used for the Common database, which is assumed to exist on a remote host. The database is set to be configured as part of the deployment environment setup (the **-dbDelayConfig "true"** command parameter is not valid in a deployment environment setup). For a complete listing of database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.
- The Windows service will be set for manual startup.
- The profile creation process will set the port values automatically (except for database-related ports). The process will validate the new profile against other profiles to ensure there are no port conflicts.

  Tip: To override the port values that the manageprofiles command-line utility will specify, use the **-portsFile** parameter. See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.
- Administrative security will be enabled.

There are two configuration options available:
- Optional: If you want all of the schema user IDs and tables to be created as part of the profile creation, you must provide a user ID that has SYSDBA privileges in the Oracle database. This ID is used to create the schemas and tables, but is not persisted anywhere in the configuration.
- Optional: If you do not want to provide the SYSDBA user ID, you can export the scripts and execute them manually.

  For both of these options, you can select a specific schema user ID for each of the components.

Table 93 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 93. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.wbiserver" (must be fully qualified)
-profileName	"*my_WPSDMGR_DE_profile*"

Table 93. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"true"
-topologyPattern	"Reference"
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-dbUserId	"*sys_user_id*" (Must be a SYSDBA user ID for deployment environments)
-dbPassword	"*sys_pwd*"
-dbDriverType	"oracle_thin"
-dbHostName	"*remote_host_name*"
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"

Table 94 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 94. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WPSDMGR_DE_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
Windows -winserviceCheck	"true"
Windows -winserviceAccountType	"localsystem"
Windows -winserviceStartupType	"manual"
Windows -winserviceUserName	"Administrator"
-dbDelayConfig	"false" (true is not valid for deployment environments)
-dbOutputScriptDir	"*install_root*\profiles\ *my_WPSDMGR_DE_profile*\dbscripts\"

WebSphere Enterprise Service Bus example

Here is a similar example that creates a WebSphere Enterprise Service Bus deployment manager profile called *my_WESBDMGR_DE_profile*.

Table 95 on page 280 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 95. Specified manageprofiles command-line utility parameters

Parameter	Value
-create	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.esbserver" (must be fully qualified)
-profileName	"*my_WESBDMGR_DE_profile*"
-enableAdminSecurity	"true"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"true"
-topologyPattern	"Reference"
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-dbUserId	"*sys_user_id*" (Must be a SYSDBA user ID for deployment environments)
-dbPassword	"*sys_pwd*"
-dbDriverType	"oracle_thin"
-dbHostName	"*remote_host_name*"
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"

Table 96 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 96. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-profilePath	"*install_root*\profiles\ *my_WESBDMGR_DE_profile*"
-hostName	"*host_name*"
-nodeName	"*host_name*CellManager*node_number*"
-cellName	"*host_name*Cell*cell_number*"
`Windows` -winserviceCheck	"true"
`Windows` -winserviceAccountType	"localsystem"
`Windows` -winserviceStartupType	"manual"
`Windows` -winserviceUserName	"Administrator"
-dbDelayConfig	"false" (true is not valid for deployment environments)
-dbOutputScriptDir	"*install_root*\profiles\ *my_WESBDMGR_DE_profile*\dbscripts\"

manageprofiles parameters for Common database configuration (per database product):

You use specific manageprofiles command-line utility parameters to configure the Common database. Parameters you specify can differ depending on the database product you are using and on the type of profile you are creating.

The tables in this topic show the manageprofiles parameters available to configure the Common database using any supported database product. Parameters associated with Common database configuration generally have a "**-db**" prefix; for example **-dbType**, and **-dbDelayConfig**. Also shown are the equivalent field names for the parameters as they appear in the Profile Management Tool.

For a complete list of manageprofiles parameters, including default values, see the topic "manageprofiles parameters" on page 377. Example manageprofiles commands used to create or augment various types of profiles can be viewed in the topics "Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 255 and "Augmenting profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 342.

To view available parameters for database configuration, choose your database product from the following list:
- "On Derby Embedded or Derby Embedded 40"
- "On Derby Network Server or Derby Network Server 40" on page 282
- "On DB2 Universal" on page 283
- "On DB2 Data Server" on page 284
- "On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)" on page 285
- "On DB2 for z/OS v8 and DB2 for z/OS v9" on page 286
- "On Oracle" on page 288
- "On Informix Dynamic Server" on page 289
- "On Microsoft SQL Server" on page 290

Note that only the **-dbType** and **-dbJDBCClasspath** parameters are available for custom profiles. This is because you are simply identifying the type and driver location for the Common database used by the deployment manager to which you will federate the custom profile.

On Derby Embedded or Derby Embedded 40

Table 97 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server profile on Derby Embedded or Derby Embedded 40.

Table 97. Available manageprofiles parameters for configuration of Common database using Derby Embedded or Derby Embedded 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
For stand-alone server profiles	
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name

Table 97. Available manageprofiles parameters for configuration of Common database using Derby Embedded or Derby Embedded 40 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbCommonForME (for Derby Embedded 40 only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be true)	N/A
-dbDelayConfig (for Derby Embedded 40 only)	Delay execution of database scripts (must select if using a remote database)
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbType	Choose a database product
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On Derby Network Server or Derby Network Server 40

Table 98 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on Derby Network Server or Derby Network Server 40.

Table 98. Available manageprofiles parameters for configuration of Common database using Derby Network Server or Derby Network Server 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbType	Choose the database product used on the deployment manager
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
For stand-alone server or deployment manager profiles	
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be true)	N/A

Table 98. Available manageprofiles parameters for configuration of Common database using Derby Network Server or Derby Network Server 40 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig (for Derby Network Server 40 only)	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 Universal

Table 99 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on DB2 Universal.

Table 99. Available manageprofiles parameters for configuration of Common database using DB2 Universal

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name

Table 99. Available manageprofiles parameters for configuration of Common database using DB2 Universal (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbDriverType	N/A
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 Data Server

Table 100 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on DB2 Universal.

Table 100. Available manageprofiles parameters for configuration of Common database using DB2 Data Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	

Table 100. Available manageprofiles parameters for configuration of Common database using DB2 Data Server (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)

Table 101 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on a database supplied with an i5/OS or IBM i operating system.

Table 101. Available manageprofiles parameters for configuration of Common database using a database supplied with an i5/OS or IBM i operating system

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files

Table 101. Available manageprofiles parameters for configuration of Common database using a database supplied with an i5/OS or IBM i operating system (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be true)	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName (for Toolbox driver, you need to specify the remote database host name)	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database collection name
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 for z/OS v8 and DB2 for z/OS v9

Table 102 on page 287 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on DB2 for z/OS v8 or DB2 for z/OS v9.

Table 102. Available manageprofiles parameters for configuration of Common database using DB2 for z/OS v8 or DB2 for z/OS v9

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbConnectionLocation	Connection location
-dbCreateNew (must always be false)	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database alias name
-dbServerPort	Server port
-dbStorageGroup	Storage group name
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On Oracle

Table 103 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on Oracle.

Table 103. Available manageprofiles parameters for configuration of Common database using Oracle

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files You must install the `ojdbc6.jar` driver to access the Oracle database. **Note:** Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle web site.
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be false)	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbDriverType	JDBC driver type
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Common database password
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	Common database user name
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
-dbLocation (required only if -dbDelayConfig is set to true)	Directory of database server installation

Table 103. Available manageprofiles parameters for configuration of Common database using Oracle (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbSysPassword	Password
-dbSysUserId	System administrator user name
N/A	Override the destination directory for generated scripts

On Informix Dynamic Server

Table 104 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on Informix Dynamic Server.

Table 104. Available manageprofiles parameters for configuration of Common database using Informix Dynamic Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbInstance (required only if **-dbDelayConfig** is set to false)	Instance name
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbLocation (required only if **-dbDelayConfig** is set to false)	Directory of database server installation
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication

Table 104. Available manageprofiles parameters for configuration of Common database using Informix Dynamic Server (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbServerPort	Server port
-dbProviderType	Required for Informix using IBM DB2 JDBC Universal driver or Informix using IBM JCC driver
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On Microsoft SQL Server

Table 105 on page 291 shows the manageprofiles parameters that are available to configure the Common database that is used by a stand-alone server, deployment manager, or custom profile on Microsoft SQL Server. Three JDBC drivers are available for this database: DataDirect Connect JDBC (XA) 3.5 build 37 (type 4), IBM WebSphere embedded Connect JDBC (XA) 3.5 build 37 (type 4), and Microsoft SQL Server JDBC Driver, version 1.2. The driver names that are displayed on the Database Configuration page are Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft).

Note: Support for the Microsoft SQL Server JDBC Driver, version 1.2 was added in WebSphere Process Server, version 6.2.0.1.

If you plan to use Microsoft SQL Server 2005 with a standalone profile, and will put the messaging engine tables in the Common Database, then you must perform the following steps:

1. Manually add four schemas to the Common database before creating stand-alone server profiles. These schemas are *XXX*SS00, *XXX*SA00, *XXX*CM00, and *XXX*BM00, where *XXX* is the first three characters of the name of the Common database.

2. Pass the `dbCommonForME=true` parameter during profile creation. The following command configures the Messaging Engines on SQL Server with the schemas that were defined above. The command uses the `dbUserId` and `dbPassword` that you specified for CommonDB.

   ```
   C:\WebSphereND\bin\manageprofiles.bat" -create -templatePath "C:\WebSphereND\
   profileTemplates\default.wbiserver" -dbHostName LNIDDBTUMSQL21 -
   dbServerPort 1433 -dbDelayConfig
   true -configureBSpace true -ceiDbName EVENT  -dbType MSSQLSERVER_Microsoft -
   dbUserId
   wpcdbadmin -dbJDBCClasspath "C:\Program Files\Microsoft SQL Server\JDBC\
   sqljdbc_1.2\enu"
   -dbName WPRCSDB -dbPassword qlwiddj23 -ceiDbServerName LNIDDBTUMSQL21 -dbCommonForME=true
   ```

Table 105. Available manageprofiles parameters for configuration of Common database using Microsoft SQL Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	Common database user name
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
-dbServerName	Database server name
-saPassword	Admin user password
-saUser	Admin user name
N/A	Override the destination directory for generated scripts

manageprofiles parameters for Common Event Infrastructure database configuration (per database product):

You use specific manageprofiles command-line utility parameters to configure the Common Event Infrastructure database used by a stand-alone server profile. Parameters you specify can differ depending on the database product you are using.

The tables in this topic show the manageprofiles parameters available to configure the Common Event Infrastructure database using any supported database product. Also shown are the equivalent field names for the parameters as they appear in the Profile Management Tool. You configure the Common Event Infrastructure database using the manageprofiles command-line utility only for stand-alone server profiles. Configuration of this database for use by deployment manager profiles must be done through the administrative console or scripting. See the topic Configuring the event database for more information.

For a complete list of manageprofiles parameters, including default values, see the topic "manageprofiles parameters" on page 377. Example manageprofiles commands used to create or augment various types of profiles can be viewed in the topics "Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 255 and "Augmenting profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 342.

To view available parameters for database configuration, choose your database product from the following list:
- "On Derby Embedded or Derby Embedded 40"
- "On Derby Network Server or Derby Network Server 40" on page 293
- "On DB2 Universal" on page 293
- "On DB2 Data Server" on page 294
- "On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)" on page 295
- "On DB2 for z/OS v8 and DB2 for z/OS v9" on page 296
- "On Oracle" on page 297
- "On Informix Dynamic Server" on page 298
- "On Microsoft SQL Server" on page 299

On Derby Embedded or Derby Embedded 40

Table 106 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Derby Embedded or Derby Embedded 40.

Table 106. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Derby Embedded or Derby Embedded 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig (for Derby Embedded 40 only)	Delay execution of database scripts (must select if using a remote database)
-ceiDbName	Common Event Infrastructure database name
-dbType	Choose a database product
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)

Table 106. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Derby Embedded or Derby Embedded 40 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
N/A	Override the destination directory for generated scripts

On Derby Network Server or Derby Network Server 40

Table 107 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Derby Network Server or Derby Network Server 40.

Table 107. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Derby Network Server or Derby Network Server 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig (for Derby Network Server 40 only)	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On DB2 Universal

Table 108 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on DB2 Universal.

Table 108. Available manageprofiles parameters for configuration of Common Event Infrastructure database using DB2 Universal

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)

Table 108. Available manageprofiles parameters for configuration of Common Event Infrastructure database using DB2 Universal (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On DB2 Data Server

Table 109 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on DB2 Data Server.

Table 109. Available manageprofiles parameters for configuration of Common Event Infrastructure database using On DB2 Data Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)

Table 110 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on the database supplied with an i5/OS or IBM i operating system.

Table 110. Available manageprofiles parameters for configuration of Common Event Infrastructure database using a database supplied with an i5/OS or IBM i operating system

Parameter	Related field on Database Configuration pages in Profile Management Tool
-ceiDbAlreadyConfigured	N/A (command-line only)
-ceiOverrideDataSource	N/A (command-line only)
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.

Table 110. Available manageprofiles parameters for configuration of Common Event Infrastructure database using a database supplied with an i5/OS or IBM i operating system (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database collection name
N/A	Override the destination directory for generated scripts

On DB2 for z/OS v8 and DB2 for z/OS v9

Table 111 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on DB2 for z/OS v8 or DB2 for z/OS v9.

Table 111. Available manageprofiles parameters for configuration of Common Event Infrastructure database using DB2 for z/OS v8 or DB2 for z/OS v9

Parameter	Related field on Database Configuration pages in Profile Management Tool
-ceiBufferPool4k	N/A (command-line only)
-ceiBufferPool8k	N/A (command-line only)
-ceiBufferPool16k	N/A (command-line only)
-ceiDbName	Common Event Infrastructure database name
-ceiDiskSizeInMB	N/A (command-line only)
-ceiOverrideDataSource	N/A (command-line only)
-dbConnectionLocation	Connection location
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication

Table 111. Available manageprofiles parameters for configuration of Common Event Infrastructure database using DB2 for z/OS v8 or DB2 for z/OS v9 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database alias name
-dbStorageGroup	Storage group name
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
N/A	Override the destination directory for generated scripts

On Oracle

Table 112 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Oracle.

Table 112. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Oracle

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbSysPassword	Password
-dbSysUserId	System administrator user name
-dbUserId	Common database user name
-ceiInstancePrefix **Note:** Deprecated in 6.2 for all databases except Informix, Oracle, Microsoft SQL Server.	N/A (command-line only)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files You must install the `ojdbc6.jar` driver to access the Oracle database. **Note:** Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle web site.
-dbLocation (required only if -dbDelayConfig is set to true)	Directory of database server installation

Table 112. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Oracle (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On Informix Dynamic Server

Table 113 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Informix Dynamic Server.

Table 113. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Informix Dynamic Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbLocation (required only if **-dbDelayConfig** is set to false)	Directory of database server installation
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbInstance	Instance name
-dbUserId	User name to authenticate with the database
-ceiInstancePrefix **Note:** Deprecated in 6.2 for all databases except Informix, Oracle, Microsoft SQL Server.	N/A (command-line only)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On Microsoft SQL Server

Table 114 shows the manageprofiles parameters that are available to configure the Common database that is used by a stand-alone server, deployment manager, or custom profile on Microsoft SQL Server. Three JDBC drivers are available for this database: DataDirect Connect JDBC (XA) 3.5 build 37 (type 4), IBM WebSphere embedded Connect JDBC (XA) 3.5 build 37 (type 4), and Microsoft SQL Server JDBC Driver, version 1.2. The driver names that are displayed on the Database Configuration page are Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft).

Note: Support for the Microsoft SQL Server JDBC Driver, version 1.2 was added in WebSphere Process Server, version 6.2.0.1.

Table 114. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Microsoft SQL Server.

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbInstallDir (required only if **-dbDelayConfig** is set to true)	N/A (command-line only)
-ceiDbName	Common Event Infrastructure database name
-dbUserId	Common database user name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbInstance (required only if **-dbDelayConfig** is set to true)	Instance name

Table 114. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Microsoft SQL Server. (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-ceiDbUser **Note:** This user must be different from the **dbUserId**. **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	CEI database user name
-ceiDbPassword **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	CEI database password
-ceiInstancePrefix **Note:** Deprecated in 6.2 for all databases except Informix, Oracle, Microsoft SQL Server.	N/A (command-line only)
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
-ceiSaPassword **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	Admin user password
-ceiSaUser **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	Admin user name
N/A	Override the destination directory for generated scripts

Augmenting profiles

You can augment an existing profile for WebSphere Application Server version 7.0 or WebSphere Application Server Network Deployment version 7.0 to add support for WebSphere Enterprise Service Bus or WebSphere Process Server, or you can augment a WebSphere Enterprise Service Bus version 7.0 profile to add support for WebSphere Process Server. Use the instructions in this topic to augment profiles interactively by using the Profile Management Tool graphical user interface (GUI) or, from a command line, by using the manageprofiles command-line utility.

Before you begin

- See the list of prerequisites for creating or augmenting profiles in the topic "Prerequisites for creating or augmenting profiles" on page 189.
- Ensure that the profile has the following characteristics:
  - It exists on a system with a WebSphere Process Server installation.
  - It is not federated to a deployment manager. You cannot use the Profile Management Tool or the manageprofiles command-line utility to augment federated profiles.
  - It does not have running servers.

About this task

If you have existing WebSphere Application Server or WebSphere Application Server Network Deployment profiles on your system, you might want the operating environments defined by those profiles to have WebSphere ESB or WebSphere Process Server functionality. Likewise, if you have existing WebSphere Enterprise Service Bus profiles, you might want them to have WebSphere Process Server functionality.

Restrictions:
- You cannot augment deployment manager profiles using the **Deployment environment** profile augmentation option.
- You cannot use the Profile Management Tool to augment profiles on WebSphere Process Server installations on 64-bit architectures except on the Linux on zSeries platform. To augment profiles on other 64-bit architectures, you can use the manageprofiles command-line utility. For information about using the manageprofiles command-line utility, see "Augmenting profiles using the manageprofiles command-line utility" on page 340. You can also use the Profile Management Tool on these architectures if you use a WebSphere Process Server 32-bit installation.

Procedure

Decide whether to augment the profile interactively by using the Profile Management Tool, or from a command line by using the manageprofiles command-line utility.
- To augment profiles by using the Profile Management Tool, see the topic "Augmenting profiles using the Profile Management Tool."
- To augment profiles by using the manageprofiles command-line utility, see the topic "Augmenting profiles using the manageprofiles command-line utility" on page 340.

Augmenting profiles using the Profile Management Tool

Use the Profile Management Tool to augment WebSphere Application Server version 7.0, WebSphere Application Server Network Deployment version 7.0, or WebSphere Enterprise Service Bus version 7.0 profiles into WebSphere Process Server profiles.

Before you begin

Ensure that the following prerequisites are satisfied:
- The profile type you will augment to (stand-alone server, deployment manager, or custom) is the same as the type of the profile from which you will augment.
- You have reviewed the list of prerequisites for creating or augmenting profiles at "Prerequisites for creating or augmenting profiles" on page 189.
- You have shut down any servers associated with the profile you plan to augment.
- If you plan to augment a stand-alone server or custom profile, you ensured that it is *not* federated to a deployment manager.
- Solaris When you use the Profile Management Tool with the Motif graphical user interface on the Solaris operating system, the default size of the Profile Management Tool might be too small to view all the messages and buttons of the Profile Management Tool. To fix the problem, add the following lines to the *install_root*/.Xdefaults file:

```
Eclipse*spacing:0
Eclipse*fontList:-misc-fixed-medium-r-normal-*-10-100-75-75-c-60-iso8859-1
```

After adding the lines, run the following command before starting the Profile Management Tool:

```
xrdb -load user_home/.Xdefaults
```

Procedure

1. Start the WebSphere Process Server Profile Management Tool.

   Use one of the following commands:

   - Linux   UNIX   *install_root*/bin/ProfileManagement/pmt.sh

   - Windows   *install_root*\bin\ProfileManagement\pmt.bat

   See the topic "Starting the Profile Management Tool" on page 199 for other methods of starting this tool.

   The Welcome page is displayed.

2. In the Welcome page, click the **Launch Profile Management Tool** button or the **Profile Management Tool** tab.

   The **Profiles** tab is displayed.

3. In the **Profiles** tab, highlight the profile you want to augment and click **Augment**.

   The **Profiles** tab lists the profiles that exist on your system. For this procedure, it is assumed you are augmenting an existing profile. If you want to create a new profile, see the topic "Creating profiles using the Profile Management Tool" on page 197.

   Restrictions:
   - You cannot augment WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus version 6.2 profiles into WebSphere Process Server version 7.0 profiles.
   - You cannot augment cell stand-alone server, management administrative agent, management job manager, or secure proxy profiles.
   - If you augment a WebSphere Application Server or WebSphere Application Server Network Deployment profile, it must be from the version of WebSphere Application Server on which WebSphere Process Server is installed. The **Augment** button is cannot be selected unless a profile can be augmented.

   The Augment Selection page opens in a separate window.

4. In the Augment Selection page, select the type of augmentation you want to apply to the profile. Then click **Next**.

   The Profile Augmentation Options page is displayed.

5. In the Profile Augmentation Options page, choose to perform a **Typical**, an **Advanced**, or (for custom profiles) a **Deployment environment** profile augmentation, and click **Next**.

   The **Typical** option augments a profile with default configuration settings.

   The **Advanced** option lets you specify your own configuration values for a profile.

   The **Deployment environment** option lets you specify your own configuration values for a custom profile and choose the cluster or clusters to apply to the managed node.

Restriction: The Profile Management Tool displays a warning message if any of the following conditions occur:

- The profile you selected to augment has a running server. You cannot augment the profile until you stop the server or click **Back** and choose another profile that does not have running servers.
- The profile you selected to augment is federated. You cannot augment a federated profile. You must click **Back** and choose another profile that is not federated.
- The profile you selected to augment is already augmented with the product you selected. You must click **Back** and choose another profile to augment.

6. Before continuing to the next page in the Profile Management Tool, proceed to one of the following topics to configure and complete augmentation of your profile.

Type of profile augmentation you selected	Procedure to complete profile augmentation based on your profile type (stand-alone server, deployment manager, or custom)
Typical	- "Augmenting **Typical** stand-alone server profiles" on page 305 - "Augmenting **Typical** deployment manager profiles" on page 313 - "Augmenting **Typical** custom profiles (managed nodes)" on page 318
Advanced	- "Augmenting **Advanced** stand-alone server profiles" on page 307 - "Augmenting **Advanced** deployment manager profiles" on page 315 - "Augmenting **Advanced** custom profiles (managed nodes)" on page 320
Deployment environment	- "Augmenting **Deployment environment** custom profiles (managed nodes)" on page 324

Results

You are ready to configure your profile, which will define an extended operating environment of the type you specified (stand-alone server, deployment manager, or custom).

Starting the Profile Management Tool:

Before you start the Profile Management Tool, be aware of the restrictions and ensure that certain prerequisites are met. You can start the Profile Management Tool in several ways, depending on the platform on which it is running.

Restrictions:

- You cannot use the Profile Management Tool to create or augment profiles on WebSphere Process Server installations on 64-bit architectures except on the Linux on zSeries platform. To create profiles on other 64-bit architectures, you can use the manageprofiles command-line utility. For information about using the manageprofiles command-line utility, see "Creating profiles using the

manageprofiles command-line utility" on page 253. You can also use the Profile Management Tool on these architectures if you use a WebSphere Process Server 32-bit installation.

- **Vista** **Windows 7** **Restriction for nonadministrative users with multiple instances:** If you install multiple instances of WebSphere Process Server as the root user and give a nonadministrative user access to only a subset of those instances, the Profile Management Tool does not function correctly for the nonadministrative user. In addition, a `com.ibm.wsspi.profile.WSProfileException` or `Access is denied` message occurs in the `install_root`\bin\ProfileManagement\pmt.bat file. By default, nonadministrative users do not have access to the `Program Files` directory, which is the default installation location for the product. To resolve this issue, nonadministrative users can install the product or be given permission to access the other product instances.

Linux **UNIX** **Windows** The language of the Profile Management Tool is determined by the default language on the system. If the default language is not one of the supported languages, then English is used. You can override the default language by starting the Profile Management Tool from the command line and using the java `user.language` setting to replace the default language. Run the following command:

- **Linux** **UNIX** `install_root`/java/bin/java `-Duser.language=locale` `install_root`/bin/ProfileManagement/startup.jar
- **Windows** `install_root`\java\bin\java `-Duser.language=locale` `install_root`\bin\ProfileManagement\startup.jar

For example, to start the Profile Management Tool in the German language on a Linux system, type the following command:

`install_root`/java/bin/java `-Duser.language=de` `install_root`/ \
bin/ProfileManagement/startup.jar

Starting the tool on all platforms

Start the tool on any platform from the First steps console. See "Starting the First steps console" on page 58 for how to start the First steps console.

Starting the tool on Linux and UNIX platforms

Linux **UNIX** You can start the tool on Linux and UNIX platforms by running the command `install_root`/bin/ProfileManagement/pmt.sh

Linux On Linux platforms only, you can also use operating system menus to start the Profile Management Tool. For example, click `Linux_operating_system_menus_to_access_programs` > IBM WebSphere > `your_product` > Profile Management Tool.

Starting the tool on Windows platforms

Windows You can use the following methods to start the tool on Windows platforms:

- Use the Windows Start menu. For example, select **Start > Programs** *or* **All Programs > IBM WebSphere > Process Server 7.0 > Profile Management Tool**.
- Run the command `install_root`\bin\ProfileManagement\pmt.bat

Augmenting Typical stand-alone server profiles:

Learn how to use the **Typical** option of the Profile Management Tool to augment and configure WebSphere Process Server or WebSphere Enterprise Service Bus stand-alone server profiles. Selecting the **Typical** option augments profiles with default configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to augment profiles and are following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301. As a result, it is assumed that you have started the Profile Management Tool, have chosen to augment a stand-alone server profile, and have selected the **Typical** profile augmentation option.

About this task

In this type of configuration, the Profile Management Tool performs the following tasks:

- Gives option to deploy the administrative console.
- If you are augmenting a profile that has security enabled, lets you enable administrative security on the WebSphere Process Server or WebSphere Enterprise Service Bus profile you are creating.
- Sets the Common Event Infrastructure and Common database configurations to Derby Embedded (if they are not already configured on the profile you are augmenting).
- If you are augmenting a profile that has security enabled, configures Business Space powered by WebSphere using Derby Embedded (if it is not already configured).
- If you are augmenting a profile that has security enabled, creates a sample Business Process Choreographer configuration for the profile.

Restriction: If you plan to federate the stand-alone server profile to a deployment manager, do not use the **Typical** option to create it. The default values for messaging engine storage and database type provided in a **Typical** profile augmentation are not suitable deployment environment installations. Use the **Advanced** option to augment the profile instead. See "Augmenting **Advanced** stand-alone server profiles" on page 307 for instructions.

As a result of following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301, you are viewing the Administrative Security page, the Profile Summary page, or the Database Security page.

Procedure

1. The page you see displayed in the Profile Management Tool depends on whether security is enabled and databases are configured on that profile.

State of security and databases on profile	First step
• Administrative security *is* enabled on the profile you are augmenting.	The Administrative Security page is displayed. Proceed to step 2 on page 306.

State of security and databases on profile	First step
• Administrative security is *not* enabled on the profile you are augmenting. • You do *not* have databases already configured.	The Profile Summary page is displayed. Proceed to step 3.
• Administrative security is *not* enabled on the profile you are augmenting. • You *do* have databases already configured.	A password page asks for the database user name and password used to configure the databases. Enter the information and click **Next**. The Profile Summary page is displayed. Proceed to step 3.

2. Enable administrative security.

    If you see this page, the profile you are augmenting has security enabled. You must re-enter the administrative user ID and password for that profile.

    If the profile you are augmenting has the WebSphere Application Server sample application deployed, it requires an account under which to run. Supply the password for the account. You cannot change the user name of the account.

    Important: If you want the Profile Management Tool to create a Business Process Choreographer sample configuration, the profile you are augmenting must have security enabled.

    The Profile Summary page is displayed.

3. In the Profile Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

    When the profile augmentation is complete, the Profile Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

    Attention: If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

    *   **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
    *   **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

    The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

4. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to start the server.

Results

You have completed one of the following tasks:

*   Augmented a WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus profile into a WebSphere Process Server profile.
*   Augmented a WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere Enterprise Service Bus profile.

The node within the profile has a server named `server1` on Linux, UNIX, and Windows platforms. The server number is incremented if there is more than one product installation.

What to do next

Check the server operation by selecting **Start the server** from the First steps console. An output window opens. If you see a message like the following one, your server is operating properly:

```
ADMU3000I: Server server1 open for e-business; process id is 3348
```

You can also check server operation by running the Installation Verification Test (IVT) from the First steps console or running the wbi_ivt command-line utility. This test is to verify that your deployment manager or stand-alone server installation is operating properly. For a stand-alone server profile, it also runs a System Health check and generates a report.

Augmenting Advanced stand-alone server profiles:

Learn how to use the **Advanced** option of the Profile Management Tool to augment and configure WebSphere Process Server or WebSphere Enterprise Service Bus stand-alone server profiles. Selecting the **Advanced** option augments profiles with customized configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to augment profiles and are following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301. As a result, it is assumed that you have started the Profile Management Tool, have chosen to augment a stand-alone server profile, and have selected the **Advanced** profile augmentation option.

About this task

By selecting the **Advanced** option, you can perform the following tasks:
- Configure the Common Event Infrastructure.
- Configure the Common database.
- If you are augmenting a profile that has security enabled, enable administrative security on the WebSphere Process Server or WebSphere Enterprise Service Bus profile you are creating.
- If you are augmenting a profile that has security enabled, configure Business Space powered by WebSphere using Derby Embedded.
- Configure Business Rules Manager.
- If you are augmenting a profile that has security enabled, create a Business Process Choreographer sample configuration.
- Configure the databases using a database design file.

Important: The procedure in this topic outlines all the pages available in the Profile Management Tool to configure an Advanced stand-alone server profile. If particular components, such as the Common database or Business Space, are already configured on the profile you are augmenting, configuration pages for those components will not appear.

Important: If you plan to federate the profile to a deployment manager, do not select the file store option for the messaging engines or Derby Embedded or Derby Embedded 40 for the Common Event Infrastructure, Business Process

Choreographer, or Common databases. The file store option and Derby Embedded or Derby Embedded 40 database cannot be used in a deployment environment configuration.

As a result of following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301, one of the following pages is displayed: the Administrative Security page, the Business Process Choreographer Configuration page, or the Business Space Configuration page.

Procedure

1. The page you see displayed in the Profile Management Tool depends on whether the profile you are augmenting has security enabled and on the profile type to which you are augmenting.

Profile type you are augmenting to and security status of existing profile you are augmenting	First step
• WebSphere Process Server or WebSphere Enterprise Service Bus profile • Security *is* enabled on the profile you are augmenting.	The Administrative Security page is displayed. Proceed to step 2.
• WebSphere Process Server profile • Security *is not* enabled on the profile that you are augmenting	The Business Process Choreographer Configuration page is displayed. Proceed to step 3.
• WebSphere Enterprise Service Bus profile • Security *is not* enabled on the profile that you are augmenting	The Business Space Configuration page is displayed. Proceed to step 4.

2. Enable administrative security.

   If you see this page, the profile you are augmenting has security enabled. You must re-enter the administrative user ID and password for that profile.

   If the profile you are augmenting has the WebSphere Application Server sample application deployed, it requires an account under which to run. Supply the password for the account. You cannot change the user name of the account.

   The Business Process Choreographer Configuration page is displayed.

3. Choose whether to create a Business Process Choreographer sample configuration.

   Restriction: Do not create a Business Process Choreographer sample configuration if you plan to use this component in a production environment or federate this stand-alone server profile to a deployment manager. The sample configuration is for development use only. For instructions on how to set up this component in a production setting, see the topics under Configuring Business Process Choreographer.

   To create a sample configuration, select the **Configure a sample Business Process Choreographer** check box and click **Next**.

   The Business Space Configuration page is displayed.

4. On the Business Space Configuration page, select the **Configure Business Space** check box to set up Business Space powered by WebSphere, an integrated user experience for application users across the IBM WebSphere business process management portfolio. If you want to configure Lotus

Webform Server to work with Human Task Management widgets in Business Space, select the **Configure Lotus Webform Server** check box and enter the Webform Server translator and installation root. Then click **Next**. Configuring Business Space sets up an integrated GUI for the business users of your application for this profile.

Important: Business Space is supported with the following database products: Derby Embedded or Derby Embedded 40, Derby Network Server or Derby Network Server 40, DB2 Universal, DB2 for i5/OS (DB2 for IBM i), DB2 for z/OS, Oracle, and Microsoft SQL Server 2005 and 2008.

If the database you use for WebSphere Process Server does not match the supported databases for Business Space, a Derby Embedded database is selected for the Business Space configuration. You cannot federate this profile into a deployment environment later, because Derby Embedded is not supported for deployment environments.

The Business Rules Manager Configuration page is displayed.

5. Select whether to configure a Business Rules Manager for the installation and then click **Next**. Business Rules Manager is a Web application that customizes the business rules templates for your business application needs.

   The next step depends on whether multiple servers are defined on your system and, if not, on whether databases are already configured on your system.

Condition	Next step
• Multiple servers *are* defined on your system.	The Application Scheduler Configuration page is displayed. Proceed to step 6.
• Multiple servers are *not* defined on your system. • Databases are *not* already defined on your system.	The Database Design page is displayed. Proceed to step 7.
• Multiple servers are *not* defined on your system. • Databases *are* already defined on your system.	A password page asks for the database user name and password used to configure the databases. Enter the information and click **Next**. The Profile Summary page is displayed. Proceed to step 9 on page 310.

6. **For Advanced profile augmentation when profile has multiple servers defined:** In the Application Scheduler Configuration page, select the server you want from the drop-down list and click **Next**. The next step depends on whether databases are already defined on your system.

Condition of databases	Next step
• Databases are *not* already defined on your system.	The Database Design page is displayed. Proceed to step 7.
• Databases *are* already defined on your system.	A password page asks for the database user name and password used to configure the databases. Enter the information and click **Next**. The Profile Summary page is displayed. Proceed to step 9 on page 310.

7. Optional: Configure the databases using a design file. This option is available for both Advanced stand-alone server and Advanced deployment manager profiles.

a. Select **Use a database design file for database configuration**.

b. Click **Browse**.

c. Specify the fully qualified path name for the design file.

d. Click **Next**.

If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating the database design file using the database design tool" on page 431.

8. In the Database Configuration page, configure both the Common database and the database used by the Common Event Infrastructure component used by selected WebSphere Process Server and WebSphere Enterprise Bus components.

Refer to the "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240 topic for details and return to this step when you have completed the fields on the Database Configuration page and the Database Configuration (Part 2) page.

The Profile Summary page is displayed.

9. In the Profile Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

When the profile augmentation is complete, the Profile Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

Attention: If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

- **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
- **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

10. Complete the stand-alone server profile configuration by performing one of the following tasks, depending on whether you must manually configure the Common Event Infrastructure and Common databases.

- If you completed configuration of the Common Event Infrastructure and Common databases using the Profile Management Tool, ensure **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to start the server.
- If you chose to postpone actual database configuration by producing scripts to be run manually, perform the following steps:

  a. Clear the check box beside **Launch the First steps console** and click **Finish** to close the Profile Management Tool. Also, close the Profiles page, which is open in a separate window.

  b. Use your site's standard database definition tools and procedures to edit and run the scripts the Profile Management Tool generated to create, or create and configure, the `event`, `eventcat`, and `WPRCSDB` databases (or their equivalents if they have different names on your system). You identified the location for these scripts in step 2 on page 241 of the topic

"Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240. Also see the topics that describe manually creating new databases or new tables in existing databases:

– For the Common Event Infrastructure database: Configuring the event database and its subtopics.

– For the Common database: "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417.

When the databases are configured, start the First steps console associated with the profile, as described in "Starting the First steps console" on page 58.

11. If you plan to use the Business Process Choreographer component in your environment, you might need your DBA to create and configure the Business Process Choreographer database.

For more information, see the topics under Configuring Business Process Choreographer.

Results

You have completed one of the following tasks:

- Augmented a WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus profile into a WebSphere Process Server profile.

- Augmented a WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere Enterprise Service Bus profile.

If you used the default server name, the node within the profile has a server named server1 for Linux, UNIX, and Windows platforms and the number is incremented if there is more than one product installation.

What to do next

Check server operation by selecting **Start the server** from the First steps console. An output window opens. If you see a message like the following message, your server is operating properly:

```
ADMU3000I: Server server1 open for e-business; process id is 3348
```

You can also check server operation by running the Installation Verification Test (IVT) from the First steps console or running the wbi_ivt command-line utility. This test is to verify that your deployment manager or stand-alone server installation is operating properly. For a stand-alone server profile, it also runs a System Health check and generates a report.

Federating stand-alone server profiles to a deployment manager:

Learn how to use the **addNode** command to federate a stand-alone server profile into a deployment manager cell. After federation, a node agent process is created. Both this node agent and the server process are managed by the deployment manager. If you federate a stand-alone server profile and include all of its applications, the act of federation installs the applications on the deployment manager. A stand-alone server profile can be federated only if there are no other federated profiles.

Before you begin

Ensure that the following prerequisites are met:

- You have installed WebSphere Process Server and created a WebSphere Process Server deployment manager.
- The deployment manager has been augmented into a WebSphere Process Server deployment manager. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.
- The stand-alone server profile is a WebSphere Process Server profile.
- The stand-alone server profile does not use file store or Derby Embedded data store for its messaging engines. If you created the profile using the **Typical** option in the Profile Management Tool, the profile uses these options. You cannot federate it to a deployment manager.
- The stand-alone server uses a database driver that supports remote access, such as Derby Network or Java toolbox JDBC.
- The deployment manager is running. If it is not, start it either by selecting **Start the deployment manager** from its First steps console or by entering the following command, where *profile_root* represents the installation location of the deployment manager profile:

  – `Linux` `UNIX` *profile_root*`/bin/startManager.sh`

  – `Windows` *profile_root*`\bin\startManager.bat`
- The stand-alone server is *not* running. If it is, stop it either by selecting **Stop the server** from its First steps console or by entering the following command, where *profile_root* represents the installation location of the stand-alone server profile:

  – `Linux` `UNIX` *profile_root*`/bin/stopServer.sh`

  – `Windows` *profile_root*`\bin\stopServer.bat`
- The deployment manager is at the same release level or higher than the profile you created or augmented.
- The deployment manager has a JMX administrative port enabled. The default protocol is SOAP.
- No other nodes are federated to the deployment manager.

If you federate a stand-alone server profile when the deployment manager is not running or is not available for other reasons, profile federation fails and the resulting profile is unusable. You must then move this stand-alone server profile directory out of the profile repository before creating another profile with the same profile name.

About this task

Perform this task when you have an existing stand-alone server profile and you need to add the capabilities that network deployment offers to that server (central management or clustering). This function provides a growth path for an existing stand-alone server profile. However, you are limited to a single cluster configuration for this deployment environment. See Single cluster topology for a description of the single cluster pattern.

Perform this task once for each cell and only for the first profile federated to the cell. Do not perform this task if the cell already has federated nodes. When you

create an environment where you do not have an existing stand-alone server profile, create the environment using custom profiles. See "Creating profiles" on page 196 for information about creating custom profiles.

Procedure

1. Go to the `bin` directory of the stand-alone server profile you want to federate. Open a command window and go to one of the following directories, depending on platform, where *profile_root* represents the installation location of the stand-alone server profile:

   - `Linux` `UNIX` `profile_root/bin`

   - `Windows` `profile_root\bin`

2. Issue the addNode command.

   Issue one of following commands if security is not enabled. The port parameter is optional and can be omitted if you used the default port numbers when creating the deployment manager profile:

   - `Linux` `UNIX` `./addNode.sh` *deployment_manager_host* *deployment_manager_SOAP_port* `-includeapps -includebuses`

   - `Windows` `addNode.bat` *deployment_manager_host* *deployment_manager_SOAP_port* `-includeapps -includebuses`

   Issue one of the following commands if security is enabled:

   - `Linux` `UNIX` `./addNode.sh` *deployment_manager_host* *deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication* `-localusername` *localuserID_for_authentication* `-localpassword` *localpassword_for_authentication* `-includeapps -includebuses`

   - `Windows` `addNode.bat` *deployment_manager_host* *deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication* `-localusername` *localuserID_for_authentication* `-localpassword` *localpassword_for_authentication* `-includeapps -includebuses`

   An output window opens. If you see a message like the following one, your stand-alone server profile was federated successfully:

   ```
   ADMU0003I: Node DMNDID2Node02 has been successfully federated.
   ```

Results

The stand-alone server profile is federated into the deployment manager. For more information about the addNode command and its parameters, see the topic Using wsadmin scripting to run the addNode command in the WebSphere Application Server Network Deployment information center.

Augmenting Typical deployment manager profiles:

Learn how to use the **Typical** option of the Profile Management Tool to augment and configure WebSphere Process Server or WebSphere Enterprise Service Bus deployment manager profiles. Selecting the **Typical** option augments profiles with default configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to augment profiles and are following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301. As a result, it is assumed that you have started

the Profile Management Tool, have chosen to augment a deployment manager profile, and have selected the **Typical** profile augmentation option.

About this task

In this type of configuration, the Profile Management Tool performs the following tasks:

- If you are augmenting a profile that has security enabled, lets you enable administrative security on the WebSphere Process Server or WebSphere Enterprise Service Bus profile you are creating.
- Sets the Common database configuration to Derby Network Server (if it is not already configured on the profile you are augmenting).

As a result of following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301, you are viewing the Administrative Security page, the Profile Summary page, or the Database Security page

Procedure

1. The page you see in the Profile Management Tool depends on whether administrative security is enabled on the profile.

State of security and databases on profile	First step
• Administrative security *is* enabled on the profile you are augmenting.	The Administrative Security page is displayed. Proceed to step 2.
• Administrative security is *not* enabled on the profile you are augmenting. • You do *not* have databases already configured.	The Profile Summary page is displayed. Proceed to step 3.
• Administrative security is *not* enabled on the profile you are augmenting. • You *do* have databases already configured.	A password page asks for the database user name and password used to configure the databases. Enter the information and click **Next**. The Profile Summary page is displayed. Proceed to step 3.

2. Enable administrative security.

   If you see this page, the profile you are augmenting has security enabled. You must re-enter the administrative user ID and password for that profile.

   The Profile Summary page is displayed.

3. In the Profile Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

   When the profile augmentation is complete, the Profile Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

   Attention: If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

   - **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
   - **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

4. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console start the server.

5. If you plan to use the Business Process Choreographer component in your environment, you must configure it. You might need your database administrator to create and configure the Business Process Choreographer database.

   For more information, see the topics under Configuring Business Process Choreographer.

Results

You have completed one of the following tasks:

- Augmented a WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus profile into a WebSphere Process Server profile.
- Augmented a WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere Enterprise Service Bus profile.

The node defined by the profile has a deployment manager named `Dmgr`.

What to do next

Check the server operation by selecting **Start the deployment manager** from the First steps console. An output window opens. If you see a message like the following one, your deployment manager is operating properly:

```
ADMU3000I: Server dmgr open for e-business; process id is 3072
```

In a deployment environment, you must create and configure other databases, create custom profiles, and federate them to your deployment manager, create servers, create clusters if you want workload management capabilities, and perform other tasks specific to your planned installation environment. Your planned environment dictates which tasks you must perform and the order in which you perform them.

For more information about planning your installation, see the topics in the *Planning the Installation, version 7.0* PDF. To learn more about the databases required by WebSphere Process Server, see the topics under *Configuring WebSphere Process Server > Configuring databases* in the *Installing and Configuring WebSphere Process Server for Multiplatforms, version 7.0* PDF. Alternatively, view the topics in the WebSphere Process Server online information center.

Augmenting Advanced deployment manager profiles:

Learn how to use the **Advanced** option of the Profile Management Tool to augment and configure WebSphere Process Server or WebSphere Enterprise Service Bus deployment manager profiles. Selecting the **Advanced** option augments profiles with customized configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to augment profiles and are following the procedure in "Augmenting profiles using the Profile

Management Tool" on page 301. As a result, it is assumed that you have started the Profile Management Tool, have chosen to augment a deployment manager profile, and have selected the **Advanced** profile augmentation option.

About this task

By selecting the **Advanced** option, you can perform the following tasks:
- Configure the Common database.
- Configure the database using a database design file.
- If you are augmenting a profile that has security enabled, enable administrative security on the WebSphere Process Server or WebSphere Enterprise Service Bus profile you are creating.

Important: The procedure in this topic outlines all the pages available in the Profile Management Tool to configure an Advanced deployment manager profile. If a particular component, such as the Common database, is already configured on the profile you are augmenting, the configuration page for that component will not appear.

As a result of following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301, one of the following pages is displayed: the Administrative Security page, the Database Design page, or the Database Security page.

Procedure

1. The page you see in the Profile Management Tool depends on whether administrative security is enabled on the profile and on whether the Common database is already configured.

State of security and database on profile	First step
• Administrative security *is* enabled on the profile you are augmenting.	The Administrative Security page is displayed. Proceed to step 2.
• Administrative security is *not* enabled on the profile you are augmenting. • You do *not* have the Common database already configured.	The Database Design page is displayed. Proceed to step 3.
• Administrative security is *not* enabled on the profile you are augmenting. • You *do* have the Common database already configured.	A password page asks for the database user name and password used to configure the database. Enter the information and click **Next**. The Profile Summary page is displayed. Proceed to step 5 on page 317.

2. Enable administrative security.

   If you see the Administrative Security page, the profile you are augmenting has security enabled. You must reenter the administrative user ID and password for that profile.

   The Database Configuration page is displayed.

3. Optional: Configure the database using a design file. This option is available for both Advanced stand-alone server and Advanced deployment manager profiles.

   a. Select **Use a database design file for database configuration**.
   b. Click **Browse**.
   c. Specify the fully qualified path name for the design file.

d. Click **Next**.

If you choose to specify a design file, the database configuration panels in the Profile Management Tool are skipped. Instead, the design file location is passed to the command line to complete the database configuration. For more information on using a design file for database configuration, see "Creating the database design file using the database design tool" on page 431.

4. In the Database Configuration page, configure the Common database used by the selected product components.

   See the topic "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240 for details and return to this step when you have completed the fields on the Database Configuration and Database Configuration (Part 2) pages. The Profile Summary page is displayed.

5. In the Profile Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

   When the profile augmentation is complete, the Profile Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

   Attention: If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

   - **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
   - **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

   The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

6. Complete the profile configuration by doing one of the following tasks, depending on whether you must manually configure the Common database.

   - If you completed configuration of the Common database using the Profile Management Tool, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to start the deployment manager.
   - If you decided to postpone actual database configuration by producing scripts to be run manually, perform the following steps:

     a. Clear the check box beside **Launch the First steps console** and click **Finish** to close the Profile Management Tool. Also, close the Profiles page, which is open in a separate window.

     b. Use your site's standard database definition tools and procedures to edit and run the scripts the Profile Management Tool generated to create or create and configure the WPRCSDB database (or its equivalent if it has a different name on your system). You identified the location for this script in step 2 on page 241 of the topic "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240. Also see the topics that describe manually creating a new Common database or tables in an existing Common database in "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417

page 417. When you have completed configuring the databases, start the First steps console associated with the profile, as instructed in "Starting the First steps console" on page 58.

Results

You have completed one of the following tasks:
- Augmented a WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere ESB profile into a WebSphere Process Server profile.
- Augmented a WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere ESB profile.

What to do next

Check server operation by selecting **Start the deployment manager** from the First steps console. An output window opens. If you see a message like the following one, your deployment manager is operating properly:

```
ADMU3000I: Server dmgr open for e-business; process id is 3072
```

In a deployment environment, you must create and configure other databases, create custom profiles, and federate them to your deployment manager, create servers, create clusters if you want workload management capabilities, and perform other tasks specific to your planned installation environment. Your planned environment dictates which tasks you must perform and the order in which you perform them.

For more information about planning your installation, see the topics in the *Planning the Installation, version 7.0* PDF. To learn more about the databases required by WebSphere Process Server, see the topics under *Configuring WebSphere Process Server > Configuring databases* in the *Installing and Configuring WebSphere Process Server for Multiplatforms, version 7.0* PDF. Alternatively, view the topics in the WebSphere Process Server online information center.

Augmenting Typical custom profiles (managed nodes):

Learn how to use the **Typical** option of the Profile Management Tool to augment and configure WebSphere Process Server or WebSphere Enterprise Service Bus custom profiles. Selecting the **Typical** option augments profiles with default configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to augment profiles and are following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301. As a result, it is assumed that you have started the Profile Management Tool, have chosen to augment a custom profile, and have selected the **Typical** profile augmentation option.

About this task

In this type of configuration, you can choose to federate the node to an existing deployment manager during the augmentation process, or federate it later using the addNode command. If you decide to federate the profile during the augmentation process, the tool sets the Common database configuration to the

same database as the deployment manager. If you decide not to federate, the database configuration is left unconfigured.

As a result of following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301, the Federation page is displayed.

Procedure
1. In the Federation page, choose to federate the node into the deployment manager now as part of the profile augmentation, or at a later time and apart from profile augmentation.
   - If you choose to federate the node as part of the profile augmentation, specify the host name or IP address and SOAP port of the deployment manager, and an authentication user ID and password if administrative security is enabled on the deployment manager. Leave the **Federate this node later** check box deselected. Then click **Next**.

     The Profile Management Tool verifies that the deployment manager exists and can be contacted, and that the authentication user ID and password are valid for that deployment manager (if it is secured).

     Attention: Federate the custom node during profile augmentation only if all the following conditions are true:
     - You do not plan to use this custom node as a migration target.
     - No other node is being federated. (Node federation must be serialized.)
     - The deployment manager is running.
     - The deployment manager is a WebSphere Process Server deployment manager. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.
     - The deployment manager is at a release level the same or higher than the release level of the custom profile you are augmenting.
     - The deployment manager has a JMX administrative port enabled. The default protocol is SOAP. (Click **System administration > Deployment manager > Administration services** in the administrative console of the deployment manager to verify the preferred connector type.)

     If you attempt to federate a custom node when the deployment manager is not running or is not available for other reasons, a warning box prevents you from continuing. If this warning box appears, click **OK** to exit from it, and then make different selections on the Federation page.
   - If you choose to federate the node at a later time and apart from profile augmentation, select the **Federate this node later** check box and click **Next**.

     See "Federating custom nodes to a deployment manager" on page 233 for more information about how to federate a node by using the addNode command. Read more about this command in the Using wsadmin scripting to run the addNode command topic in the WebSphere Application Server Network Deployment information center.

   The Profile Summary page is displayed.
2. In the Profile Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

   When the profile augmentation is complete, the Profile Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

Attention: If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

- **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
- **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

3. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console access the product documentation.

Results

You have completed one of the following tasks:

- Augmented a WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus profile into a WebSphere Process Server profile.
- Augmented a WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere Enterprise Service Bus profile.

What to do next

If you did not federate the profile during profile augmentation, federate it now. The node within the profile is empty until you federate the node and use the deployment manager to customize the node.

Augmenting Advanced custom profiles (managed nodes):

Learn how to use the **Advanced** option of the Profile Management Tool to augment and configure WebSphere Process Server or WebSphere Enterprise Service Bus custom profiles. Selecting the **Advanced** option augments profiles with customized configuration settings.

Before you begin

This topic assumes that you are using the Profile Management Tool to augment profiles and are following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301. As a result, it is assumed that you have started the Profile Management Tool, have chosen to augment a custom profile, and have selected the **Advanced** profile augmentation option.

About this task

While augmenting custom profiles, you can choose to federate the node to an existing deployment manager during the augmentation process, or federate it later using the addNode command.

As a result of following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301, you are viewing the Federation page.

Procedure

1. In the Federation page, choose to federate the node into the deployment manager now as part of the profile augmentation, or at a later time and apart from profile augmentation.

   - If you choose to federate the node as part of the profile augmentation, specify the host name or IP address and SOAP port of the deployment manager, and an authentication user ID and password (if administrative security is enabled on the deployment manager). Leave the **Federate this node later** check box deselected. Then click **Next**.

     The Profile Management Tool verifies that the deployment manager exists and can be contacted, and that the authentication user ID and password are valid for that deployment manager (if it is secured).

     Important:

     Do *not* federate the custom node during profile augmentation if any one of the following situations is true:

     – You plan to use this custom node as a migration target.
     – Another profile is being federated. (Node federation must be serialized.)
     – The deployment manager is not running or you are not sure if it is running.
     – The deployment manager has not yet been augmented into a WebSphere Process Server deployment manager.
     – The deployment manager is not at a release level the same or higher than the release level of the custom profile you are creating or augmenting.
     – The deployment manager does not have a JMX administrative port enabled.
     – The deployment manager is reconfigured to use the non-default remote method invocation (RMI) as the preferred Java Management Extensions (JMX) connector. (Select **System administration > Deployment manager > Administration services** in the administrative console of the deployment manager to verify the preferred connector type.)

     If you attempt to federate a custom node when the deployment manager is not running or is not available for other reasons, a warning box prevents you from continuing. If this warning box appears, click **OK** to exit from it, and then make different selections on the Federation page.

   - If you choose to federate the node at a later time and apart from profile augmentation, select the **Federate this node later** check box and click **Next**.

     See "Federating custom nodes to a deployment manager" on page 233 for more information about how to federate a node by using the addNode command. Read more about this command in the Using wsadmin scripting to run the addNode command topic in the WebSphere Application Server Network Deployment information center.

   The Database Configuration page is displayed.

2. In the Database Configuration page, perform the following steps:

   a. Review the database product. The database that matches the database used on the deployment manager to which this custom profile will be federated is displayed.

   b. Provide the location (directory) of the JDBC driver class path files for the database. You can accept the default values for Derby Network Server, Derby Network Server 40 or DB2 Universal Database.

c. Click **Next**.

The Profile Summary page is displayed.

3. In the Profile Summary page, click **Augment** to augment the profile, or **Back** to change the characteristics of the profile.

When the profile augmentation is complete, the Profile Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

Attention: If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

*   **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
*   **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

4. In the Profile Complete page, ensure **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to access product documentation.

Results

You have completed one of the following tasks:

*   Augmented a WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus profile into a WebSphere Process Server profile.
*   Augmented a WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere Enterprise Service Bus profile.

What to do next

The node within the profile is empty until you federate it and use the administrative console to customize it.

In a deployment environment, you must create and configure databases, create other custom profiles and federate them to your deployment manager, create servers, create clusters if you want workload management capabilities, and perform other tasks specific to your planned installation environment. Your planned environment dictates which tasks you must perform and the order in which you perform them.

For more information about planning your installation, see the topics in the *Planning the Installation, version 7.0* PDF. To learn more about the databases required by WebSphere Process Server, see the topics under *Configuring WebSphere Process Server > Configuring databases* in the *Installing and Configuring WebSphere Process Server for Multiplatforms, version 7.0* PDF. Alternatively, view the topics in the WebSphere Process Server online information center.

Federating custom nodes to a deployment manager:

You can use the addNode command to federate a custom node into a deployment manager cell. The following instructions guide you through the process of federating and deploying custom nodes.

Before you begin

Before using this procedure, ensure that the following prerequisites are met:
- You have installed WebSphere Process Server and created a WebSphere Process Server deployment manager and a custom profile. This procedure assumes you did *not* federate the custom profile during its creation or augmentation, either with the Profile Management Tool or with the manageprofiles command-line utility.
- The deployment manager is running. If it is not, start it either by selecting **Start the deployment manager** from its First steps console or by entering the following command, where *profile_root* represents the installation location of the deployment manager profile:
  - `Linux` `UNIX` *profile_root*/bin/startManager.sh
  - `Windows` *profile_root*\bin\startManager.bat
- The deployment manager has been augmented into a WebSphere Process Server deployment manager. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager.
- The deployment manager is at the same release level or higher than the custom profile you created or augmented.
- The deployment manager has a JMX administrative port enabled. The default protocol is SOAP.
- You do not plan to use this custom node as a migration target.

About this task

Federate a custom node so that it can be managed by a deployment manager. Use the addNode command to federate a custom profile into a deployment manager cell.

Procedure
1. Go to the `bin` directory of the custom profile you want to federate. Open a command window and go to one of the following directories (from a command line), depending on platform (where *profile_root* represents the installation location of the custom profile):
   - `Linux` `UNIX` *profile_root*/bin
   - `Windows` *profile_root*\bin
2. Issue the addNode command.

   Issue one of the following commands from the command line if security is not enabled:
   - `Linux` `UNIX` ./addNode.sh *deployment_manager_host deployment_manager_SOAP_port*
   - `Windows` addNode.bat *deployment_manager_host deployment_manager_SOAP_port*

Issue one of the following commands from the command line if security is enabled:

- `Linux`   `UNIX`   `./addNode.sh` *deployment_manager_host* *deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication*

- `Windows`   `addNode.bat` *deployment_manager_host* *deployment_manager_SOAP_port* `-username` *userID_for_authentication* `-password` *password_for_authentication*

An output window opens. If you see a message similar to the following message, your custom profile was federated successfully:

`ADMU0003I: Node DMNDID2Node03 has been successfully federated.`

Results

The custom profile is federated into the deployment manager. For more information about the addNode command and its parameters, see the topic Using wsadmin scripting to run the addNode command in the WebSphere Application Server Network Deployment information center.

What to do next

After federating the custom profile, go to the administrative console of the deployment manager to customize the empty node or to create a new server.

Augmenting Deployment environment custom profiles (managed nodes):

Learn how to use the **Deployment environment** option of the Profile Management Tool to augment and configure WebSphere Process Server or WebSphere Enterprise Service Bus custom profiles. Selecting the **Deployment environment** option lets you configure a profile with customized configuration values to be used in an existing deployment environment pattern.

Before you begin

This topic assumes that you are using the Profile Management Tool to augment profiles and are following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301. As a result, it is assumed that you have started the Profile Management Tool, have chosen to augment a custom profile, and have selected the **Deployment environment** profile augmentation option.

About this task

Select the **Deployment environment** profile augmentation option to set up a fully configured profile for your deployment environment. This option configures and installs all components needed for WebSphere Process Server to work. The following components are configured as part of this option:

- Business Process Choreographer
- Common Event Infrastructure
- Business Rules Manager
- Service Component Architecture

In this type of configuration, you can perform the following tasks:

- Federate the node to an existing deployment manager, which has a deployment environment pattern already defined.
- Specify the clusters to define on that deployment environment, as well as your own values for the Common database configuration.

As a result of following the procedure in "Augmenting profiles using the Profile Management Tool" on page 301, you are viewing the Federation page.

Procedure

1. In the Federation page, you must federate the node into the deployment manager now as part of the profile augmentation. The **Federate this node later** check box does not appear on the Federation page for this type of profile augmentation. Specify the host name or IP address and SOAP port of the deployment manager, and an authentication user ID and password. Then click **Next**.

   To find the SOAP port number of the deployment manager, go to the *dmgr_profile_root*/logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".

   The Profile Management Tool verifies that the deployment manager exists and can be contacted, and that the authentication user ID and password are valid for that deployment manager. It also validates that there is a valid deployment environment defined on the deployment manager, and retrieves the pattern and database type back from the deployment manager.

   If you attempt to federate a custom node when the deployment manager is not running or is not available for other reasons, a warning box prevents you from continuing. If this warning box appears, click **OK** to exit from it, cancel this profile augmentation, and make the necessary changes to your system.

   The Deployment Environment Configuration page is displayed.

2. In the Deployment Environment Configuration page, select at least one cluster to assign this node to on the deployment environment pattern and click **Next**. The page offers one to three clusters based on the deployment environment pattern defined previously on the deployment manager:

Table 115. Clusters offered per deployment environment pattern on existing deployment manager

Deployment environment pattern on deployment manager	Clusters offered
Remote messaging and remote support	• **Application deployment target**: consists of a cluster to which user applications need to be deployed. • **Messaging infrastructure**: consists of a cluster where messaging engines are located. • **Support infrastructure**: consists of a cluster that hosts the Common Event Infrastructure server and other infrastructure services that are used to manage your system.

Table 115. Clusters offered per deployment environment pattern on existing deployment manager (continued)

Deployment environment pattern on deployment manager	Clusters offered
Remote messaging	• **Application deployment target**: consists of a cluster to which user applications need to be deployed. With a remote messaging deployment environment pattern, the application deployment target cluster also assumes the functionality of the supporting infrastructure cluster. • **Messaging infrastructure**: consists of a cluster where bus members are located.
Single cluster	• **Application deployment target**: consists of a cluster to which user applications need to be deployed. With a single cluster deployment environment pattern, the application deployment target cluster also assumes the functionality of the messaging and the supporting infrastructure clusters.

See the following topics for more information:
- Topology types and deployment environment patterns. A deployment environment pattern specifies the constraints and requirements of the components and resources involved in a deployment environment. The patterns are designed to meet the needs of most business requirements and are intended to help you create a deployment environment in the most straightforward way.
- Functions of IBM-supplied deployment environment patterns. To design a robust deployment environment, you need to understand the functionality each cluster can provide in a particular IBM-supplied deployment environment pattern or a custom deployment environment. This knowledge can help you make the correct decisions as to which deployment environment pattern best meets your needs.

The Database Configuration page is displayed.

3. In the Database Configuration page, perform the following steps:

    a. Review the database product. The database that matches the database used on the deployment manager to which this custom profile will be federated is displayed.

    Note: Derby Network Server, Derby Network Server 40, DB2 for i5/OS (Toolbox), and DB2 for IBM i (Toolbox) can be accessed both locally and remotely.

    b. Provide the location (directory) of the JDBC driver class path files for the database. You can accept the default values for Derby Network Server, Derby Network Server 40, and DB2 Universal Database.

    c. Click **Next**.

    The Profile Summary page is displayed.

4. In the Profile Summary page, click **Augment** to augment the profile or **Back** to change the characteristics of the profile.

When the profile augmentation is complete, the Profile Complete page is displayed with the message **The Profile Management tool augmented the profile successfully**.

Attention: If errors are detected during profile augmentation, other messages might appear in place of the success message, for example:

- **The Profile Management tool augmented the profile but errors occurred**, which indicates that profile augmentation completed but errors were generated.
- **The Profile Management tool cannot augment the profile**, which indicates that profile augmentation failed completely.

The Profile Complete page identifies the log file to reference in order to troubleshoot the problems.

5. In the Profile Complete page, ensure that **Launch the First steps console** is selected and click **Finish** to exit. Also, close the Profiles page, which is open in a separate window. Use the First steps console to access product documentation.

Results

You have completed one of the following tasks:

- Augmented a WebSphere Application Server, WebSphere Application Server Network Deployment, or WebSphere Enterprise Service Bus profile into a WebSphere Process Server profile.
- Augmented a WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere Enterprise Service Bus profile.

What to do next

Use the deployment manager to customize the node. You might add more custom nodes if not all the cluster members are assigned.

Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool:

Selected WebSphere Process Server components require a database, called the *Common* database, and a Common Event Infrastructure local database to operate. Using values you provide on the Database Configuration pages, the Profile Management Tool automatically creates the Common database and, for stand-alone server profiles, the Common Event Infrastructure database on a local system. It also creates all required tables. You must configure these databases to have a working installation.

Before you begin

This procedure assumes that you have started the Profile Management Tool and have chosen to create or augment a profile through either the Advanced or Deployment environment profile creation or augmentation option. You are performing the procedure in one of the following topics:

- "Creating **Advanced** stand-alone server profiles" on page 202
- "Augmenting **Advanced** stand-alone server profiles" on page 307
- "Creating **Advanced** deployment manager profiles" on page 214
- "Augmenting **Advanced** deployment manager profiles" on page 315

- "Creating Deployment environment deployment manager profiles" on page 220

In the topic, you are at the step in the procedure that asks you to complete the Database Configuration page.

About this task

The following WebSphere Process Server components use the Common database:
- Application Scheduler
- Business rule group
- Mediation
- Recovery
- Relationship service
- Selector
- Event Sequencing (Lock Manager)
- Enterprise Service Bus Logger Mediation Primitive
- Messaging Engines (if you selected the **Use this database for Messaging Engines (MEs)** check box detailed in step 6 on page 243).

The Common Event Infrastructure component uses the Common Event Infrastructure database.

For more information about the various databases and database tables the WebSphere Process Server product uses, see Choosing a database.

Important: If you choose Derby Network Server or Derby Network Server 40 as your database product, ensure that the server is running on the host and port you specified during profile creation or augmentation, even if the database host is local. You can make sure that the server is running only after the profile is created or augmented.

Procedure
1. In the **Choose a database product** field, select the database product you want to use, or accept the default value of Derby Embedded or Derby Embedded 40 (for stand-alone server profiles) or Derby Network Server or Derby Network Server 40 (for deployment manager profiles).

   Restriction: Informix Dynamic Server and Microsoft SQL Server are not supported on deployment managers using the deployment environment configuration.
2. To store the database creation and configuration scripts that the profile creation or augmentation process creates in a location other than the default location, select the **Override the destination directory for generated scripts** check box and designate your new location in the **Database script output directory** field. The profile creation or augmentation process creates scripts that you or the database administrator can run manually to create new databases and their required tables, if you choose not to do so during profile creation or augmentation. The process creates scripts for the Common database for all profile types and scripts for the Common Event Infrastructure database for stand-alone server profiles.

   The default locations for the databases are as follows:
   - For the Common Event Infrastructure database:
     - `Linux` `UNIX` `install_root`/profiles/`profile name`/dbscripts/ `CEI_ceiDbName`

- – `Windows` `install_root\profiles\`*`profile name`*`\dbscripts\CEI_`*`ceiDbName`*
- • For the Common database:
  - – `Linux` `UNIX` `install_root/profiles/`*`profile name`*`/dbscripts/`
    `CommonDB/`*`dbType`*`/`*`dbName`*
  - – `Windows` `install_root\profiles\`*`profile name`*`\dbscripts\CommonDB\`
    `dbType``\`*`dbName`*

For selected database products, you can prevent automatic creation and configuration of databases by selecting the **Delay execution of database scripts (must select if using a remote database)** check box in this page, described in step 5 on page 243.)

3. Enter your Common database name or accept the default value.

   The name of the database on IBM i using Independent Auxiliary Storage Pools (IASPs) can be the name of the IASP.

   Default Common database names differ based on the database product:
   - • `*SYSBAS` for DB2 for i5/OS (Toolbox) and DB2 for IBM i (Toolbox)
   - • `WPRCSDB` for all other database products

   If you plan to use an existing database, this name must match the name of that database. If you plan to create a new database and the name you specify is already associated with another WebSphere Process Server profile, you must use a different database name.

   Note: This restriction does not apply to IBM i. All profiles on IBM i use the same database name.

   Note: The Oracle database name (dbName) is the Oracle Identifier (SID) and must exist in order to create tables. When creating stand-alone server profiles, it can be shared between the Common database and the Common Event Infrastructure database. It is recommended that you remove all Oracle database resources before creating a new profile, because the Common Event Infrastructure database creates unique database resources, such as table spaces, which will fail if they exist in the Oracle server.

4. **For stand-alone server profiles only:** Enter your Common Event Infrastructure database name or accept the default value.

   Restriction: This field appears only when you are creating or augmenting a stand-alone server profile.

   The name of the database on IBM i using Independent Auxiliary Storage Pools (IASPs) can be the name of the IASP.

   Default Common Event Infrastructure database names differ based on the database product:
   - • `*SYSBAS` for DB2, i5/OS (Toolbox), and DB2 for IBM i (Toolbox)
   - • `orcl` for Oracle
   - • `EVENT` for all other database products

   If you plan to use an existing database, this name must match the name of that database. If you plan to create a new database and the name you specify is already associated with another WebSphere Process Server profile, you must use a different database name.

   Note: This restriction does not apply to IBM i. All profiles on IBM i use the same database name.

5. Select the **Delay execution of database scripts (must select if using a remote database)** check box if you do not want to create and configure a local database automatically or create tables in an existing one during profile creation or augmentation. A local database will be created if this check box is not selected. If you select this option, you or the database administrator must manually run the scripts that are stored in the location specified in the **Database script output directory** field on this page.

   See the following topics for instructions on manually creating and configuring databases:

   - To create a new Common database or create tables in an existing one, see "Creating the Common database and tables after profile creation or augmentation" on page 416 or "Creating tables on an existing Common database after profile creation or augmentation" on page 417.

   - **For stand-alone server profiles only:** To create a new Common Event Infrastructure database, see Manually running database configuration scripts

   Important: Do not use the Common database scripts located in the following directories (where the variable *db_type* represents the supported database product):

   - Linux   UNIX   *install_root*/dbscripts/CommonDB/*db_type*

   - Windows   *install_root*\dbscripts\CommonDB*db_type*

   These default scripts have not been updated by the profile creation or augmentation process.

   Restriction: The **Delay execution of database scripts (must select if using a remote database)** option is not available for the following configurations:

   - If you chose the Derby Embedded, Derby Embedded 40, Derby Network Server, or Derby Network Server 40 product for any profile type.

   - If you chose to create a deployment manager using the Deployment environment option.

   The next step depends on whether you are creating or augmenting a stand-alone server or deployment manager profile.

Type of profile you are creating or augmenting	Next step
Stand-alone server	Proceed to step 6 on page 243.
Deployment manager	Proceed to step 8 on page 244.

6. **For stand-alone server profiles only:** Select the **Use a file store for Messaging Engines (MEs)** check box to use a file store for messaging engines. If you select this check box, the messaging engines are created and configured on a file store (except for the Common Event Infrastructure messaging engine, which uses a Derby Embedded or Derby Embedded 40 local database even if this option is selected). If you do not select this check box, and do not select the **Use this database for Messaging Engines (MEs)** check box detailed in step 7 on page 244, the messaging engines are created and configured on the default Derby Embedded or Derby Embedded 40 database. Derby Embedded or Derby Embedded 40 databases cannot be created on remote workstations. For more information about file stores, see Administering file stores in the WebSphere Application Server Network Deployment information center.

7. **For stand-alone server profiles only:** Select the **Use this database for Messaging Engines (MEs)** check box to use the Common database for

messaging engines. If you do not select this check box, and do not select the **Use a file store for Messaging Engines (MEs)** check box detailed in step 6 on page 243, the messaging engines are created and configured on the default Derby Embedded or Derby Embedded 40 database. Derby Embedded or Derby Embedded 40 databases cannot be created on remote workstations. For more information about data stores, see Administering data stores in the WebSphere Application Server Network Deployment information center.

Restriction: This option is not available if you chose the Derby Embedded or Derby Embedded 40 product.

Restriction: Common database cannot be used for messaging engine configuration on Informix. Do not select the **Use this database for Messaging Engines (MEs)** option for stand-alone profile creation if the Common database is Informix.

8. Click **Next**. The next step depends on the type of profile you are creating or augmenting and on the database product you chose.

Type of profile you are creating or augmenting	Next step
Stand-alone server profile with the default value of **Derby Embedded or Derby Embedded 40** selected.	The Profile Summary page is displayed. Return to step 15 on page 209 in the topic "Creating **Advanced** stand-alone server profiles" on page 202 or step 9 on page 310 in the topic "Augmenting **Advanced** stand-alone server profiles" on page 307.

Type of profile you are creating or augmenting	Next step
Stand-alone server profile with any database product other than **Derby Embedded or Derby Embedded 40** selected. Deployment manager profile with any database product selected.	The Database Configuration (Part 2) page is displayed with fields specific to the database product you selected. Review the topic "Database Configuration (Part 2) page" on page 245 for information about how to complete this page. When you have completed entering information about this page, click **Next**. The tool checks that a valid connection for the Common database exists. If the database connection does not exist, you need to correct the problem either by starting up the database or altering the specified parameters before continuing. The Profile Summary page is displayed. Depending on the topic from which you accessed this one, return to one of the following steps: • Step 15 on page 209 in the topic "Creating **Advanced** stand-alone server profiles" on page 202 • Step 9 on page 310 in the topic "Augmenting **Advanced** stand-alone server profiles" on page 307 • Step 11 on page 218 in the topic "Creating **Advanced** deployment manager profiles" on page 214 • Step 5 on page 317 in the topic "Augmenting **Advanced** deployment manager profiles" on page 315 • Step 10 on page 225 in the topic "Creating Deployment environment deployment manager profiles" on page 220

Database Configuration (Part 2) page:

When you select your database product on the Database Configuration page in the Profile Management Tool, a follow-up page, called the Database Configuration (Part 2) page, asks you for database-specific information. It contains slightly different fields and default values, depending on your database product selection.

You must complete this page even if you chose to postpone creating a new database or adding tables to an existing one by selecting the **Delay execution of database scripts** check box on the previous Database Configuration page. The values you choose on the Database Configuration (Part 2) page are added to the database configuration scripts stored in the directory you specified in the **Database script output directory** field on the previous page (or in the default directory for these scripts if you did not specify a different location).

Restriction: You cannot create a new database if you are using DB2 for z/OS V8 or V9, or Oracle. In these cases, the Common database and, for a stand-alone server profile, the Common Event Infrastructure database, must exist. If you select one of these databases, a warning message alerts you to this restriction.

Choose the link for your database product from the following list to determine how to complete the Database Configuration (Part 2) page:

- "Derby Embedded or Derby Embedded 40" on page 246
- "Derby Network Server or Derby Network Server 40" on page 247
- "DB2 Universal Database" on page 247
- "DB2 Data Server" on page 248
- "DB2 for z/OS V8 and V9" on page 248
- "DB2 for i5/OS (Toolbox) and DB2 for IBM i (Toolbox)" on page 249
- "Informix Dynamic Server" on page 250
- "Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft)" on page 250
- "Oracle" on page 251

When you have completed the Database Configuration (Part 2) page, click **Next**. The tool checks that a valid connection exists to the Common database. If the tool identifies an error, you must correct the problem before continuing by either making sure that the database is up and running or altering parameters in order to make a good connection.

The Profile Summary page is displayed. Depending on the topic from which you accessed this one, return to one of the following steps:

- Step 15 on page 209 in the topic "Creating **Advanced** stand-alone server profiles" on page 202
- Step 9 on page 310 in the topic "Augmenting **Advanced** stand-alone server profiles" on page 307
- Step 11 on page 218 in the topic "Creating **Advanced** deployment manager profiles" on page 214
- Step 5 on page 317 in the topic "Augmenting **Advanced** deployment manager profiles" on page 315
- Step 10 on page 225 in the topic "Creating Deployment environment deployment manager profiles" on page 220

Derby Embedded or Derby Embedded 40

Table 51 on page 246 lists the fields you must complete on the Database Configuration (Part 2) page when you select Derby Embedded or Derby Embedded 40 as your database product.

Important: If you choose Derby Embedded or Derby Embedded 40 as your database product, after profile creation or augmentation completes, ensure that the server is running on the host and port you specified during profile creation, even if the database host is local.

Table 116. Required database configuration fields for Derby Embedded or Derby Embedded 40

Field	Action needed
Schema name	Enter the database schema name. Default is APP.

Derby Network Server or Derby Network Server 40

Table 52 on page 247 lists the fields you must complete on the Database Configuration (Part 2) page when you select Derby Network Server or Derby Network Server 40 as your database product.

Important: If you choose Derby Network Server or Derby Network Server 40 as your database product, after profile creation or augmentation completes, ensure that the server is running on the host and port you specified during profile creation, even if the database host is local.

Table 117. Required database configuration fields for Derby Network Server or Derby Network Server 40

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1527 or enter the correct server port number.
Schema name	Enter the database schema name. Default is APP.

DB2 Universal Database

Table 53 on page 247 lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 Universal Database as your database product.

Table 118. Required database configuration fields for DB2 Universal Database

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `install_root`/universalDriver_wbi/lib on Linux and UNIX platforms, or `install_root`\universalDriver_wbi\lib on Windows platforms, or browse to the location on your system that contains the following files: • `db2jcc.jar` • `db2jcc_license_cu.jar` *or* `db2jcc_license_cisuz.jar` An error message is displayed if the files cannot be found at the specified location.

Table 118. Required database configuration fields for DB2 Universal Database (continued)

Field	Action needed
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 50000 or enter the correct server port number.
Schema name	Enter the database schema name. Default is `WPRCDB`.

DB2 Data Server

Table 54 on page 248 lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 Data Server as your database product.

Table 119. Required database configuration fields for DB2 Data Server

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `install_root`/universalDriver_wbi/lib on Linux and UNIX platforms, or `install_root`\universalDriver_wbi\lib on Windows platforms, or browse to the location on your system that contains the following files: • `db2jcc.jar` • `db2jcc_license_cu.jar` *or* `db2jcc_license_cisuz.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 50000 or enter the correct server port number.
Schema name	Enter the database schema name. Default is `WPRCDB`.

DB2 for z/OS V8 and V9

Table 55 on page 248 lists the fields you must complete on the Database Configuration (Part 2) page when you select DB2 for z/OS V8 and V9 as your database product. You cannot create a new database using these databases. The Common database and, for a stand-alone server profile, the Common Event Infrastructure database, must exist.

Table 120. Required database configuration fields for DB2 for z/OS V8 and V9

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • `db2jcc.jar` • `db2jcc_license_cisuz.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Enter the database server host name.
Server port	Accept the default value of 446 or enter the correct server port number.
Database alias name	Enter the database alias name.
Connection location	Enter the connection location.
Storage group name	Enter the storage group name.

DB2 for i5/OS (Toolbox) and DB2 for IBM i (Toolbox)

Table 56 on page 249 lists the fields you must complete on the Database Configuration (Part 2) page when you select or DB2 for IBM i (Toolbox) as your database product. This selection is also valid for DB2 for i5/OS (Toolbox).

Table 121. Required database configuration fields for DB2 for IBM i (Toolbox) or DB2 for IBM i (Toolbox)

Field	Action needed
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Accept the default value of `/QIBM/ProdData/HTTP/Public/jt400/lib` or browse to the location on your system that contains the following file: • `jt400.jar` An error message is displayed if the file cannot be found at the specified location.
Database server host name (for example IP address)	Enter the database server host name.
Database collection name	Accept the default value of `WPRCSDB` or enter the correct schema name. To prevent naming conflicts within the specified database, specify a schema name whose first three characters are unique from the names of other schemas residing in the database.

Informix Dynamic Server

Table 57 on page 250 lists the fields you must complete on the Database Configuration (Part 2) page when you select Informix Dynamic Server as your database product.

Table 122. Required database configuration fields for Informix Dynamic Server

Field	Action needed
Directory of database server installation	Indicates the database installation directory if you are using Informix databases.
User name to authenticate with the database	Enter the user name to authenticate with the database.
Password for database authentication	Enter a password to authenticate with the database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • `ifxjdbc.jar` • `ifxjdbcx.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1526 or enter the correct server port number.
Instance name	Enter the correct instance name.

Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft)

Table 58 on page 250 lists the fields you must complete on the Database Configuration (Part 2) page when you select Microsoft SQL Server (DataDirect) or Microsoft SQL Server (Microsoft) as your database product.

Table 123. Required database configuration fields for Microsoft SQL Server DataDirect and Microsoft SQL Server (Microsoft)

Field	Action needed
CEI database user name	Enter the CEI database user name.
CEI database password	Enter a password to authenticate with the CEI database.
Confirm password	Confirm the password.
Common database user name	Enter the user name to authenticate with the database.
Common database password	Enter a password to authenticate with the database.
Confirm password	Confirm the password.

Field	Action needed
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the following files: • `sqlserver.jar` • `base.jar` • `util.jar` Also, the file `spy.jar` must be available in the following location relative to the location of the JDBC driver class path files: • `Linux` `UNIX` `../spy/spy.jar` • `Windows` `..\spy\spy.jar` An error message is displayed if the files cannot be found at the specified location.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Database server name	Enter the database server name.
Server port	Accept the default value of 1433 or enter the correct server port number.
Admin user name	Enter the user ID that has privileges to create and drop databases and users or accept the default value of `sa`. This ID is required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Password	Enter the password for the user **Admin user name** ID.
Confirm password	Confirm the password.

Oracle

Table 59 on page 251 lists the fields you must complete on the Database Configuration (Part 2) page when you select Oracle as your database product. You cannot create a new database using this database.

Important: You must have a user ID that has SYSDBA privileges before creating any profile.

Table 124. Required database configuration fields for Oracle

Field	Action needed
Directory of database server installation	Enter or browse for the database server installation. Required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Business Space database user name	User ID for the Business Space database. This option only appears if BSpace is enabled.
Business Space database password	Enter a password to authenticate with the Business Space database.
Confirm password	Confirm the password.

Table 124. Required database configuration fields for Oracle (continued)

Field	Action needed
CEI database user name	User ID for the Common Event Infrastructure database.
CEI database password	Enter a password to authenticate with the Common Event Infrastructure database.
Confirm password	Confirm the password.
Common database user name	User ID for the Common database.
Password	Enter a password to authenticate with the Common database.
Confirm password	Confirm the password.
Location (directory) of JDBC driver classpath files	Enter the location on your system that contains the file `ojdbc6.jar`. You must install the `ojdbc6.jar` driver to access the Oracle database. **Important:** Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle Web site. An error message is displayed if the files cannot be found at the specified location.
JDBC driver type	Click **OCI** or **Thin**.
Database server host name (for example IP address)	Accept the default value of `localhost` or enter the correct database server host name.
Server port	Accept the default value of 1521 or enter the correct server port number.
System administrator user name	Enter the user ID that has privileges to create and drop databases and users or accept the default value of SYSUSER. Required when the **Delay execution of database scripts** option is NOT selected in the previous screen.
Password	Enter the password for the user **Admin user name** ID.
Confirm password	Confirm the password.

If you selected **Use this database for Messaging Engines (MEs)** in the first Database Configuration screen, the Database Configuration (Part 3) page is displayed. Table 60 on page 252 lists the fields you must complete.

Table 125. Required database configuration fields for using Oracle with Messaging Engines

Field	Action needed
Business Process Choreographer messaging engine	
User name	Enter the Business Process Choreographer messaging engine user ID. This option only appears if BPC is enabled.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
CEI bus messaging engine	
User name	Enter the CEI bus messaging engine user ID.

Table 125. Required database configuration fields for using Oracle with Messaging Engines (continued)

Field	Action needed
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
SCA application bus messaging engine	
User name	Enter the SCA application bus messaging engine user ID.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.
SCA system bus messaging engine	
User name	Enter the SCA system bus messaging engine user ID.
Password	Enter the password for the user ID.
Confirm password	Confirm the password.

Augmenting profiles using the manageprofiles command-line utility

Augmentation is the ability to change an existing profile with an augmentation template. You can augment existing WebSphere Application Server or WebSphere Application Server Network Deployment profiles into WebSphere Enterprise Service Bus or WebSphere Process Server profiles, or WebSphere Enterprise Service Bus profiles into WebSphere Process Server profiles. You can augment a profile from the command line using the manageprofiles command-line utility.

Before you begin

Before using this procedure, ensure that you have done the following tasks:
- You have reviewed the list of prerequisites for creating or augmenting a profile at "Prerequisites for creating or augmenting profiles" on page 189.
- You have shut down any servers associated with the profile that you plan to augment.
- If you plan to augment a stand-alone server or custom profile, you have determined if it has already been federated to a deployment manager:
  - If the profile you want to augment has already been federated to a deployment manager, you cannot augment it using the manageprofiles command-line utility.
  - If the profile you want to augment has not already been federated to a deployment manager, when you do federate it via the addNode command later, the following must be true of the deployment manager with which it is federated in order for the augmentation to complete successfully:
    - It must be running.
    - It must be at a release level the same or higher than that of the profile you are augmenting. WebSphere Process Server profiles cannot use a WebSphere Enterprise Service Bus deployment manager, but WebSphere Enterprise Service Bus profiles can use a WebSphere Process Server deployment manager. WebSphere Enterprise Service Bus profiles can use a WebSphere Enterprise Service Bus or WebSphere Process Server deployment manager.
    - It must have a JMX administrative port enabled. The default protocol is SOAP.

- It must have already been augmented into a WebSphere Process Server profile, depending on the product you have installed.
- You have reviewed example profile augmentation commands in "Augmenting profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 342 or "Augmenting profiles with manageprofiles command-line utility with Oracle database – examples" on page 348.
- You have verified that you are not already running the manageprofiles command-line utility on the same profile. If an error message is displayed, determine if there is another profile creation or augmentation action in progress. If so, wait until it completes.

Security role required for this task: See "Granting write permission of files and directories to nonroot users for profile creation" on page 193.

To use the manageprofiles command-line utility to augment a profile, perform the following steps.

Procedure

1. Determine the template that the existing profile was created with (deployment manager, stand-alone, or managed). You can determine the template that was used for creating the profile by viewing the profile registry in *install_root*/properties/profileRegistry.xml. Do not modify this file, use it only to view the templates.
2. Find the appropriate template to augment to. You can augment an existing WebSphere Application Server or WebSphere Application Server Network Deployment profile into a WebSphere Process Server or WebSphere ESB profile. You can augment an existing WebSphere ESB profile into a WebSphere Process Server profile. The following profile templates are available:
   - `default.wbiserver`: for a WebSphere Process Server stand-alone server profile, which defines a stand-alone server.
   - `dmgr.wbiserver`: for a WebSphere Process Server deployment manager profile, which defines a deployment manager. A *deployment manager* provides one administrative interface to a logical group of servers on one or more workstations.
   - `managed.wbiserver`: for a WebSphere Process Server custom profile, which, when federated to a deployment manager, defines a managed node. If you have decided that your solution requires a deployment environment, your runtime environment requires one or more managed nodes. A *custom profile* contains an empty node that you must federate into a deployment manager cell to make operational. Federating the custom profile changes it into a managed node.
   - `default.esbserver`: for a WebSphere Enterprise Service Bus stand-alone server profile, which defines a stand-alone server.
   - `dmgr.esbserver`: for a WebSphere Enterprise Service Bus deployment manager profile, which defines a deployment manager.
   - `managed.esbserver`: for a WebSphere Enterprise Service Bus custom profile, which, when federated to a deployment manager, defines a managed node.

   Use the augment parameter to make changes to an existing profile with an augmentation template. The augment parameter causes the manageprofiles command-line utility to update or augment the profile identified in the **-profileName** parameter using the template in the **-templatePath** parameter. The augmentation templates that you can use are determined by which IBM products and versions are installed in your environment. Make sure that you

specify the fully qualified file path for **-templatePath**, because a relative file path for the **-templatePath** parameter results in the specified profile not being fully augmented.

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

3. Run the file from the command line. Do not supply a **-profilePath** parameter. Here are some simple examples. For more complex examples, see "Augmenting profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" or "Augmenting profiles with manageprofiles command-line utility with Oracle database – examples" on page 348.

  - `Linux` `UNIX` `manageprofiles.sh -augment -templatePath` *install_root*/profileTemplates/default.wbiserver -profileName *MyProfileName*

  - `Windows` `manageprofiles.bat -augment -templatePath` *install_root*\ profileTemplates\default.wbiserver -profileName *MyProfileName*

If you have created a response file, use the **-response** parameter: -response myResponseFile

The following example shows a response file for an augment operation:

```
augment
profileName=testResponseFileAugment
templatePath=install_root/profileTemplates/default.wbiserver

nodeName=myNodeName
cellName=myCellName
hostName=myHostName
omitAction=myOptionalAction1, myOptionalAction2
```

The command displays status as it runs. Wait for it to finish. Normal syntax checking on the response file applies as the file is parsed like any other response file. Individual values in the response file are treated as command-line parameters.

What to do next

You can see that your profile augmentation completed successfully if you receive a `INSTCONFSUCCESS: Profile augmentation succeeded.` message, and you can check the following log file:

- `Linux` `UNIX` *install_root*/logs/manageprofiles/ *profile_name*_augment.log

- `Windows` *install_root*\logs\manageprofiles*profile_name*_augment.log

- **On i5/OS platforms:** *user_data_root*/profileRegistry/logs/manageprofiles/ *profile_name*_augment.log

Run the Installation Verification Test (IVT) tool to verify that the profile was augmented successfully. To do this, run the following command:

- **On i5/OS platforms:** *profile_root*/bin/wbi_ivt

- `Linux` `UNIX` **On Linux and UNIX platforms:** *profile_root*/bin/ wbi_ivt.sh

- `Windows` **On Windows platforms:** *profile_root*\bin\wbi_ivt.bat

Augmenting profiles with manageprofiles command-line utility with Derby or DB2 databases – examples:

Example profile augmentation commands to help you augment stand-alone server, deployment manager, and custom profiles using the manageprofiles command-line utility on your installation.

Stand-alone server profile

The following command example augments a WebSphere Application Server stand-alone server profile called *AppServ04* with WebSphere Process Server functionality on a Windows server. The parameters in Table 126 and Table 127 on page 344 specify the following:

- The Derby Embedded or Derby Embedded 40 database product will be used for both the Common and Common Event Infrastructure databases, which are set to be created and configured on the localhost during the profile augmentation process. For complete listings of database-related manageprofiles parameters, see the topics "manageprofiles parameters for Common database configuration (per database product)" on page 280 and "manageprofiles parameters for Common Event Infrastructure database configuration (per database product)" on page 291.
- A sample Business Process Choreographer implementation will *not* be created.
- Business Rules Manager will *not* be configured.
- Business Space powered by WebSphere will *not* be configured.
- Administrative security was enabled during the profile creation process and will be specified again during profile augmentation.

Table 126 shows manageprofiles command-line utility parameters with example values used to create a stand-alone server profile.

Table 126. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\ default.wbiserver" (must be fully qualified)
-profileName	"*AppServ04*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-dbType	"DERBY_EMBEDDED" "DERBY_EMBEDDED40"
-dbUserId	"*cei_id*"
-dbPassword	"*cei_pwd*"
-ceiDbName	"event"
-dbDelayConfig	"true"
-ceiDbAlreadyConfigured	"false"
-configureBPC	"false"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbCommonForME	"false"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-configureBSpace	"false"
-configureBRM	"false"

Table 127 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 127. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*AppServ04*\dbscripts\\CommonDB\Derby\WPRCSDB"
-dbOutputscriptDir	"*install_root*\profiles*AppServ04*\dbscripts\\CEI_event"

WebSphere Enterprise Service Bus example

Here is a similar example that augments a WebSphere Application Server stand-alone server profile called *AppServ03* with WebSphere Enterprise Service Bus functionality.

Table 128 shows manageprofiles command-line utility parameters with example values used to create a stand-alone server profile.

Table 128. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\\default.esbserver" (must be fully qualified)
-profileName	"*AppServ03*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-dbType	"DERBY_EMBEDDED" "DERBY_EMBEDDED40"
-dbUserId	"*cei_id*"
-dbPassword	"*cei_pwd*"
-ceiDbName	"event"
-dbDelayConfig	"true"
-ceiDbAlreadyConfigured	"false"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbCommonForME	"false"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-configureBSpace	"false"

Table 129 on page 345 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 129. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*AppServ03*\dbscripts\CommonDB\Derby\WPRCSDB"
-dbOutputscriptDir	"*install_root*\profiles*AppServ03*\dbscripts\CEI_event"

Deployment manager profile (without deployment environment setup)

The following command example augments a WebSphere Application Server deployment manager profile called *Dmgr02* with WebSphere Process Server functionality on a Windows server. The parameters in Table 130 and Table 131 on page 346 specify the following:

- The Derby Network Server or Derby Network Server 40 database product will be used for the Common database, which is set to be created and configured on the localhost during the profile augmentation process. For a complete listing of database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.
- Administrative security was enabled during the profile creation process and will be specified again during profile augmentation.

Table 130 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 130. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\dmgr.wbiserver" (must be fully qualified)
-profileName	"*Dmgr02*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false" (configuration of a deployment environment is not supported during profile augmentation)
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbDelayConfig	"false"
-dbHostName	"localhost"
-dbUserId	"*db_id*"
-dbPassword	"*db_pwd*"
-dbServerPort	"1528"

Table 131 on page 346 shows a manageprofiles command-line utility parameter with a default value that does not normally have to be changed.

Table 131. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*Dmgr02*\dbscripts\\CommonDB\Derby\WPRCSDB"

WebSphere Enterprise Service Bus example

Here is a similar example that augments a WebSphere Application Server deployment manager profile called *Dmgr04* with WebSphere Enterprise Service Bus functionality.

Table 132 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 132. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\\dmgr.esbserver" (must be fully qualified)
-profileName	"*Dmgr04*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false" (configuration of a deployment environment is not supported during profile augmentation)
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbName	"WPRCSDB"
-dbCreateNew	"true"
-dbDelayConfig	"false"
-dbHostName	"localhost"
-dbUserId	"*db_id*"
-dbPassword	"*db_pwd*"
-dbServerPort	"1529"

Table 133 shows a manageprofiles command-line utility parameter with a default value that does not normally have to be changed.

Table 133. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*Dmgr04*\dbscripts\\CommonDB\Derby\WPRCSDB"

Custom profile (without deployment environment setup)

The following command example augments a WebSphere Application Server custom profile called *Custom21* with WebSphere Process Server functionality on a Windows server. This example is set to operate with the deployment manager profile created above.

The parameters in Table 134 specify the following:
- The Derby Network Server or Derby Network Server 40 database product is used for the Common database, which is assumed to already exist. The custom profile creation simply needs to point to the database used by the deployment manager to which the custom profile will be federated. For a complete listing of database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.
- Administrative security is enabled on the deployment manager to which the custom profile will be federated.

See "manageprofiles parameters" on page 377 for a listing of all valid manageprofiles parameters.

Table 134 shows manageprofiles command-line utility parameters with example values used to create a custom profile.

Table 134. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\ managed.wbiserver" (must be fully qualified)
-profileName	"*Custom21*"
-dmgrHost	"localhost"
-dmgrPort	"8903" (To find the -dmgrPort value, go to the `dmgr_profile_root`\logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".)
-dmgrAdminPassword	"*admin_pwd*"
-dmgrAdminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbJDBCClasspath	"*install_root*\derby\lib"

WebSphere Enterprise Service Bus example

Here is a similar example that augments a WebSphere Application Server custom profile called *Custom05* with WebSphere Enterprise Service Bus functionality.

Table 135 on page 348 shows manageprofiles command-line utility parameters with example values used to create a custom profile.

Table 135. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\ managed.esbserver" (must be fully qualified)
-profileName	"*Custom05*"
-dmgrHost	"localhost"
-dmgrPort	"8902" (To find the -dmgrPort value, go to the *dmgr_profile_root*\logs directory for the deployment manager associated with this custom profile. In this directory, open the AboutThisProfile.txt file and find the value for the entry "Deployment manager SOAP connector port:".)
-dmgrAdminPassword	"*admin_pwd*"
-dmgrAdminUserName	"*admin_id*"
-ndtopology	"false"
-dbType	"DERBY_NETWORKSERVER" "DERBY_NETWORKSERVER40"
-dbJDBCClasspath	"*install_root*\derby\lib"

Augmenting profiles with manageprofiles command-line utility with Oracle database – examples:

Example profile augmentation commands to help you augment stand-alone server and deployment manager profiles using the manageprofiles command-line utility on your installation.

Stand-alone server profile

The following command example augments a WebSphere Application Server stand-alone server profile called *AppServ04* with WebSphere Process Server functionality on a Windows server. The parameters in Table 136 on page 349, Table 137 on page 349 and Table 138 on page 349 specify the following:

- The Oracle database product will be used for both the Common and Common Event Infrastructure databases, which are both assumed to already exist on the localhost. Both databases are set to be configured later (the **-dbDelayConfig "true"** command parameter value specifies that configuration scripts be created but not run). For complete listings of database-related manageprofiles parameters, see the topics "manageprofiles parameters for Common database configuration (per database product)" on page 280 and "manageprofiles parameters for Common Event Infrastructure database configuration (per database product)" on page 291.
- A sample Business Process Choreographer configuration will be created.
- Business Rules Manager will *not* be configured.
- Business Space powered by WebSphere will *not* be configured.
- Administrative security was enabled during the profile creation process and will be specified again during profile augmentation.

Table 136 on page 349 shows manageprofiles command-line utility parameters with example values used to create a stand-alone server profile.

Table 136. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\ default.wbiserver" (must be fully qualified)
-profileName	"*AppServ04*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-configureBPC	"true"
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-ceiDbName	"EVENT"
-dbDelayConfig	"true"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-dbCommonForME	"true"
-dbPassword	"*db_pwd*"
-dbDriverType	"oracle_thin"
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"
-configureBSpace	"false"
-configureBRM	"false"

Table 137 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 137. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*AppServ04*\dbscripts\"
-dbHostName	"*local_host_name*"

Table 138 shows additional manageprofiles command-line utility parameters that are not displayed via the Profile Management Tool that can be specified to select your own user name and password combinations for Oracle.

Table 138. Additional manageprofiles command-line utility parameters for Oracle

Parameter	Default values	Remarks
-dbSysUserId	"*sys_user_id*"	This ID must have SYSDBA privileges. Do not use the Oracle internal user 'sys'. This parameter is needed if you want to configure the database and its objects during profile creation [when dbDelayConfig = "FALSE"]
-dbSysPassword	"*sys_pwd*"	This parameter is needed if you want to configure the database and its objects during profile creation [when dbDelayConfig = "FALSE"]

Table 138. Additional manageprofiles command-line utility parameters for Oracle (continued)

Parameter	Default values	Remarks
-dbCommonUserId	"*common_db_userID*" (used to create Common DB objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCommonUserId is ORCCOMM
-dbCommonPassword	"*common_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCommonPassword will be set to dbPassword. For example: dbCommonPassword = dbPassword
-dbBSpaceUserId	"*bspace_db_userID*" (used to configure Business Space)	This parameter is needed if you require your own Business Space schema. If not, the default value (IBMBUSSP) will be set.
-dbBSpacePassword	"*bspace_db_pwd*" (used to configure Business Space)	This parameter is needed if you need your own Business Space password otherwise default value will be set in the following order: dbBSpacePassword = "YouNameIt" else dbBSpacePassword = dbPassword [if exists] else dbBSpacePassword = IBMBUSSP
-dbCeiUserId	"*cei_userID*" (used to create CEI objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiUserId is ORCCEID
-dbCeiPassword	"*cei_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example, dbCeiPassword = dbPassword
	All the parameters below are only valid if -dbCommonForME = "true"	
-dbBPCMeUserId	"*bpc_me_userID*" (used to create BPC ME objects) (only valid if -configureBPC = "true")	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbBPCMeUserId is ORCBM00
-dbBPCMePassword	"*bpc_me_pwd*" (only valid if -configureBPC = "true")	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example, dbBPCMePassword = dbPassword

Table 138. Additional manageprofiles command-line utility parameters for Oracle (continued)

Parameter	Default values	Remarks
-dbCeiMeUserId	"*cei_me_userID*" (used to create CEI ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiMeId is ORCCM00
-dbCeiMePassword	"*cei_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbCeiMePassword = dbPassword
-dbAppMeUserId	"*app_me_userID*" (used to create SCAAPP ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbAppMeId is ORCSA00
-dbAppMePassword	"*app_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword
-dbSysMeUserId	"*sys_me_userID*" (used to create SCASYS ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbSysMeUserId is ORCSS00
-dbSysMePassword	"*sys_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword

WebSphere Enterprise Service Bus example

Here is a similar example that augments a WebSphere Application Server stand-alone server profile called *AppServ03* with WebSphere Enterprise Service Bus functionality. The difference is the database is set to be configured now (the -dbDelayConfig "false" command parameter value specifies that configuration scripts be run).

Table 139 shows manageprofiles command-line utility parameters with example values used to create a stand-alone server profile.

Table 139. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A

Table 139. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-templatePath	"*install_root*\profileTemplates\ default.esbserver" (must be fully qualified)
-profileName	"*AppServ03*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-ceiDbName	"EVENT"
-dbDelayConfig	"false"
-fileStoreForME	"false" (cannot be true when -dbCommonForME is also true)
-dbCommonForME	"true"
-dbLocation	"*oracle_install_directory*"
-dbPassword	"*db_pwd*"
-dbDriverType	"oracle_thin"
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"
-dbSysUserId	"*sys_user_id*"
-dbSysPassword	"*sys_pwd*"
-configureBSpace	"false"

Table 140 shows manageprofiles command-line utility parameters with default values that do not normally have to be changed.

Table 140. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*AppServ03*\dbscripts\"
-dbHostName	"*local_host_name*"

Table 141 shows additional manageprofiles command-line utility parameters that are not displayed via the Profile Management Tool that can be specified to select your own user name and password combinations for Oracle.

Table 141. Additional manageprofiles command-line utility parameters for Oracle

Parameter	Default values	Remarks
-dbCommonUserId	"*common_db_userID*" (used to create Common DB objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCommonUserId is ORCCOMM

Table 141. Additional manageprofiles command-line utility parameters for Oracle (continued)

Parameter	Default values	Remarks
-dbCommonPassword	"*common_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCommonPassword will be set to dbPassword. For example: dbCommonPassword = dbPassword
-dbBSpaceUserId	"*bspace_db_userID*" (used to configure Business Space)	This parameter is needed if you require your own Business Space schema. If not, the default value (IBMBUSSP) will be set.
-dbBSpacePassword	"*bspace_db_pwd*" (used to configure Business Space)	This parameter is needed if you need your own Business Space password otherwise default value will be set in the following order: dbBSpacePassword = "YouNameIt" else dbBSpacePassword = dbPassword [if exists] else dbBSpacePassword = IBMBUSSP
-dbCeiUserId	"*cei_userID*" (used to create CEI objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiUserId is ORCCEID
-dbCeiPassword	"*cei_db_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example, dbCeiPassword = dbPassword
	All the parameters below are only valid if -dbCommonForME = "true"	
-dbCeiMeUserId	"*cei_me_userID*" (used to create CEI ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbCeiMeId is ORCCM00
-dbCeiMePassword	"*cei_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbCeiMePassword = dbPassword
-dbAppMeUserId	"*app_me_userID*" (used to create SCAAPP ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbAppMeId is ORCSA00

Parameter	Default values	Remarks
-dbAppMePassword	"*app_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword
-dbSysMeUserId	"*sys_me_userID*" (used to create SCASYS ME objects)	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, this user will be generated automatically based on Oracle Database name [SID]. For example: If SID is ORCL, dbSysMeUserId is ORCSS00
-dbSysMePassword	"*sys_me_pwd*"	This parameter is needed if you select the Custom Users and Passwords option during profile creation. For the Generate Users with Single Password option, dbCeiPassword will be set to dbPassword. For example: dbAppMePassword = dbPassword

Deployment manager profile (without deployment environment setup)

The following command example augments a WebSphere Application Server deployment manager profile called *Dmgr02* with WebSphere Process Server functionality on a Windows server. The parameters in Table 142 and Table 143 on page 355 specify the following:

- The Oracle database product will be used for the Common database, which is assumed to exist on a remote host. The database is set to be configured later (the -dbDelayConfig "true" command parameter value specifies that configuration scripts be created but not run). For a complete listing of database-related manageprofiles parameters, see the topic "manageprofiles parameters for Common database configuration (per database product)" on page 280.
- Administrative security was enabled during the profile creation process and will be specified again during profile augmentation.

Table 142 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 142. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.wbiserver" (must be fully qualified)
-profileName	"*Dmgr02*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false" (configuration of a deployment environment is not supported during profile augmentation)
-dbType	"ORACLE"

Table 142. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-dbName	"WPRCSDB"
-dbDelayConfig	"true"
-dbPassword	"*db_pwd*"
-dbDriverType	"oracle_thin"
-dbHostName	"*remote_host_name*"
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"

Table 143 shows a manageprofiles command-line utility parameter with a default value that does not normally have to be changed.

Table 143. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*Dmgr02*\dbscripts\\"

WebSphere Enterprise Service Bus example

Here is a similar example that augments a WebSphere Application Server deployment manager profile called *Dmgr04* with WebSphere Enterprise Service Bus functionality. The difference is the database is set to be configured now (the -dbDelayConfig "false" command parameter value specifies that configuration scripts be run).

Table 144 shows manageprofiles command-line utility parameters with example values used to create a deployment manager profile.

Table 144. Specified manageprofiles command-line utility parameters

Parameter	Value
-augment	N/A
-templatePath	"*install_root*\profileTemplates\ dmgr.esbserver" (must be fully qualified)
-profileName	"*Dmgr04*"
-adminPassword	"*admin_pwd*"
-adminUserName	"*admin_id*"
-ndtopology	"false" (configuration of a deployment environment is not supported during profile augmentation)
-dbType	"ORACLE"
-dbName	"WPRCSDB"
-dbDelayConfig	"false"
-dbLocation	"*oracle_install_directory*"
-dbPassword	"*db_pwd*"
-dbDriverType	"oracle_thin"
-dbHostName	"*remote_host_name*"

Table 144. Specified manageprofiles command-line utility parameters (continued)

Parameter	Value
-dbJDBCClasspath	"*oracle_library_directory*"
-dbServerPort	"1521"
-dbSysUserId	"*sys_user_id*"
-dbSysPassword	"*sys_pwd*"

Table 145 shows a manageprofiles command-line utility parameter with a default value that does not normally have to be changed.

Table 145. Defaulted manageprofiles command-line utility parameters

Parameter	Default values
-dbOutputScriptDir	"*install_root*\profiles*Dmgr04*\dbscripts\"

manageprofiles parameters for Common database configuration (per database product):

You use specific manageprofiles command-line utility parameters to configure the Common database. Parameters you specify can differ depending on the database product you are using and on the type of profile you are creating.

The tables in this topic show the manageprofiles parameters available to configure the Common database using any supported database product. Parameters associated with Common database configuration generally have a "**-db**" prefix; for example **-dbType**, and **-dbDelayConfig**. Also shown are the equivalent field names for the parameters as they appear in the Profile Management Tool.

For a complete list of manageprofiles parameters, including default values, see the topic "manageprofiles parameters" on page 377. Example manageprofiles commands used to create or augment various types of profiles can be viewed in the topics "Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 255 and "Augmenting profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 342.

To view available parameters for database configuration, choose your database product from the following list:
- "On Derby Embedded or Derby Embedded 40" on page 281
- "On Derby Network Server or Derby Network Server 40" on page 282
- "On DB2 Universal" on page 283
- "On DB2 Data Server" on page 284
- "On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)" on page 285
- "On DB2 for z/OS v8 and DB2 for z/OS v9" on page 286
- "On Oracle" on page 288
- "On Informix Dynamic Server" on page 289
- "On Microsoft SQL Server" on page 290

Note that only the **-dbType** and **-dbJDBCClasspath** parameters are available for custom profiles. This is because you are simply identifying the type and driver location for the Common database used by the deployment manager to which you will federate the custom profile.

On Derby Embedded or Derby Embedded 40

Table 97 on page 281 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server profile on Derby Embedded or Derby Embedded 40.

Table 146. Available manageprofiles parameters for configuration of Common database using Derby Embedded or Derby Embedded 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
For stand-alone server profiles	
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name
-dbCommonForME (for Derby Embedded 40 only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be true)	N/A
-dbDelayConfig (for Derby Embedded 40 only)	Delay execution of database scripts (must select if using a remote database)
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbType	Choose a database product
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On Derby Network Server or Derby Network Server 40

Table 98 on page 282 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on Derby Network Server or Derby Network Server 40.

Table 147. Available manageprofiles parameters for configuration of Common database using Derby Network Server or Derby Network Server 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	

Table 147. Available manageprofiles parameters for configuration of Common database using Derby Network Server or Derby Network Server 40 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbType	Choose the database product used on the deployment manager
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
For stand-alone server or deployment manager profiles	
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be true)	N/A
-dbDelayConfig (for Derby Network Server 40 only)	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 Universal

Table 99 on page 283 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on DB2 Universal.

Table 148. Available manageprofiles parameters for configuration of Common database using DB2 Universal

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbDriverType	N/A
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 Data Server

Table 100 on page 284 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on DB2 Universal.

Table 149. Available manageprofiles parameters for configuration of Common database using DB2 Data Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Schema name
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)

Table 101 on page 285 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on a database supplied with an i5/OS or IBM i operating system.

Table 150. Available manageprofiles parameters for configuration of Common database using a database supplied with an i5/OS or IBM i operating system

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be true)	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName (for Toolbox driver, you need to specify the remote database host name)	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database collection name
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On DB2 for z/OS v8 and DB2 for z/OS v9

Table 102 on page 287 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on DB2 for z/OS v8 or DB2 for z/OS v9.

Table 151. Available manageprofiles parameters for configuration of Common database using DB2 for z/OS v8 or DB2 for z/OS v9

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbConnectionLocation	Connection location
-dbCreateNew (must always be false)	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database alias name
-dbServerPort	Server port
-dbStorageGroup	Storage group name
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)

Table 151. Available manageprofiles parameters for configuration of Common database using DB2 for z/OS v8 or DB2 for z/OS v9 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
N/A	Override the destination directory for generated scripts

On Oracle

Table 103 on page 288 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on Oracle.

Table 152. Available manageprofiles parameters for configuration of Common database using Oracle

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files You must install the `ojdbc6.jar` driver to access the Oracle database. **Note:** Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle web site.
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew (must always be false)	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbDriverType	JDBC driver type
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Common database password

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	Common database user name
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
-dbLocation (required only if -dbDelayConfig is set to true)	Directory of database server installation
-dbSysPassword	Password
-dbSysUserId	System administrator user name
N/A	Override the destination directory for generated scripts

On Informix Dynamic Server

Table 104 on page 289 shows the manageprofiles parameters available to configure the Common database used by a stand-alone server, deployment manager, or custom profile on Informix Dynamic Server.

Table 153. Available manageprofiles parameters for configuration of Common database using Informix Dynamic Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbInstance (required only if **-dbDelayConfig** is set to false)	Instance name
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbLocation (required only if **-dbDelayConfig** is set to false)	Directory of database server installation
-dbName	Common database name

Table 153. Available manageprofiles parameters for configuration of Common database using Informix Dynamic Server (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbProviderType	Required for Informix using IBM DB2 JDBC Universal driver or Informix using IBM JCC driver
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
N/A	Override the destination directory for generated scripts

On Microsoft SQL Server

Table 105 on page 291 shows the manageprofiles parameters that are available to configure the Common database that is used by a stand-alone server, deployment manager, or custom profile on Microsoft SQL Server. Three JDBC drivers are available for this database: DataDirect Connect JDBC (XA) 3.5 build 37 (type 4), IBM WebSphere embedded Connect JDBC (XA) 3.5 build 37 (type 4), and Microsoft SQL Server JDBC Driver, version 1.2. The driver names that are displayed on the Database Configuration page are Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft).

Note: Support for the Microsoft SQL Server JDBC Driver, version 1.2 was added in WebSphere Process Server, version 6.2.0.1.

If you plan to use Microsoft SQL Server 2005 with a standalone profile, and will put the messaging engine tables in the Common Database, then you must perform the following steps:

1. Manually add four schemas to the Common database before creating stand-alone server profiles. These schemas are *XXX*SS00, *XXX*SA00, *XXX*CM00, and *XXX*BM00, where *XXX* is the first three characters of the name of the Common database.
2. Pass the `dbCommonForME=true` parameter during profile creation. The following command configures the Messaging Engines on SQL Server with the schemas that were defined above. The command uses the `dbUserId` and `dbPassword` that you specified for CommonDB.

```
C:\WebSphereND\bin\manageprofiles.bat" -create -templatePath "C:\WebSphereND\
profileTemplates\default.wbiserver" -dbHostName LNIDDBTUMSQL21 -
dbServerPort 1433 -dbDelayConfig
true -configureBSpace true -ceiDbName EVENT  -dbType MSSQLSERVER_Microsoft -
```

```
dbUserId
wpcdbadmin -dbJDBCClasspath "C:\Program Files\Microsoft SQL Server\JDBC\
sqljdbc_1.2\enu"
-dbName WPRCSDB -dbPassword qlwiddj23 -ceiDbServerName LNIDDBTUMSQL21 -dbCommonForME=true
```

Table 154. Available manageprofiles parameters for configuration of Common database using Microsoft SQL Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
For custom profiles	
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbType	Choose the database product used on the deployment manager
For stand-alone server or deployment manager profiles	
-dbCommonForME (for stand-alone server profiles only)	Use this database for Messaging Engines (MEs)
-dbCreateNew	N/A
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbName	Common database name
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	Common database user name
-fileStoreForME (for stand-alone server profiles only)	Use a file store for Messaging Engines (MEs)
-dbServerName	Database server name
-saPassword	Admin user password
-saUser	Admin user name
N/A	Override the destination directory for generated scripts

manageprofiles parameters for Common Event Infrastructure database configuration (per database product):

You use specific manageprofiles command-line utility parameters to configure the Common Event Infrastructure database used by a stand-alone server profile. Parameters you specify can differ depending on the database product you are using.

The tables in this topic show the manageprofiles parameters available to configure the Common Event Infrastructure database using any supported database product. Also shown are the equivalent field names for the parameters as they appear in the Profile Management Tool. You configure the Common Event Infrastructure database using the manageprofiles command-line utility only for stand-alone server profiles. Configuration of this database for use by deployment manager profiles must be done through the administrative console or scripting. See the topic Configuring the event database for more information.

For a complete list of manageprofiles parameters, including default values, see the topic "manageprofiles parameters" on page 377. Example manageprofiles commands used to create or augment various types of profiles can be viewed in the topics "Creating profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 255 and "Augmenting profiles with manageprofiles command-line utility with Derby or DB2 databases – examples" on page 342.

To view available parameters for database configuration, choose your database product from the following list:
- "On Derby Embedded or Derby Embedded 40" on page 292
- "On Derby Network Server or Derby Network Server 40" on page 293
- "On DB2 Universal" on page 293
- "On DB2 Data Server" on page 294
- "On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)" on page 295
- "On DB2 for z/OS v8 and DB2 for z/OS v9" on page 296
- "On Oracle" on page 297
- "On Informix Dynamic Server" on page 298
- "On Microsoft SQL Server" on page 299

On Derby Embedded or Derby Embedded 40

Table 106 on page 292 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Derby Embedded or Derby Embedded 40.

Table 155. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Derby Embedded or Derby Embedded 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig (for Derby Embedded 40 only)	Delay execution of database scripts (must select if using a remote database)
-ceiDbName	Common Event Infrastructure database name
-dbType	Choose a database product

Table 155. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Derby Embedded or Derby Embedded 40 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On Derby Network Server or Derby Network Server 40

Table 107 on page 293 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Derby Network Server or Derby Network Server 40.

Table 156. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Derby Network Server or Derby Network Server 40

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig (for Derby Network Server 40 only)	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On DB2 Universal

Table 108 on page 293 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on DB2 Universal.

Table 157. Available manageprofiles parameters for configuration of Common Event Infrastructure database using DB2 Universal

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On DB2 Data Server

Table 109 on page 294 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on DB2 Data Server.

Table 158. Available manageprofiles parameters for configuration of Common Event Infrastructure database using On DB2 Data Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication

Table 158. Available manageprofiles parameters for configuration of Common Event Infrastructure database using On DB2 Data Server (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbServerPort	Server port
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On DB2 for IBM i (Toolbox) and DB2 for i5/OS (Toolbox)

Table 110 on page 295 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on the database supplied with an i5/OS or IBM i operating system.

Table 159. Available manageprofiles parameters for configuration of Common Event Infrastructure database using a database supplied with an i5/OS or IBM i operating system

Parameter	Related field on Database Configuration pages in Profile Management Tool
-ceiDbAlreadyConfigured	N/A (command-line only)
-ceiOverrideDataSource	N/A (command-line only)
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files

Table 159. Available manageprofiles parameters for configuration of Common Event Infrastructure database using a database supplied with an i5/OS or IBM i operating system (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database collection name
N/A	Override the destination directory for generated scripts

On DB2 for z/OS v8 and DB2 for z/OS v9

Table 111 on page 296 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on DB2 for z/OS v8 or DB2 for z/OS v9.

Table 160. Available manageprofiles parameters for configuration of Common Event Infrastructure database using DB2 for z/OS v8 or DB2 for z/OS v9

Parameter	Related field on Database Configuration pages in Profile Management Tool
-ceiBufferPool4k	N/A (command-line only)
-ceiBufferPool8k	N/A (command-line only)
-ceiBufferPool16k	N/A (command-line only)
-ceiDbName	Common Event Infrastructure database name
-ceiDiskSizeInMB	N/A (command-line only)
-ceiOverrideDataSource	N/A (command-line only)
-dbConnectionLocation	Connection location
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files

Table 160. Available manageprofiles parameters for configuration of Common Event Infrastructure database using DB2 for z/OS v8 or DB2 for z/OS v9 (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-dbPassword	Password for database authentication
-cdbSchemaName A new parameter that take precedence over dbSchemaName if both are specified.-dbSchemaName **Note:** Deprecated in V7.	Database alias name
-dbStorageGroup	Storage group name
-dbType	Choose a database product
-dbUserId	User name to authenticate with the database
N/A	Override the destination directory for generated scripts

On Oracle

Table 112 on page 297 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Oracle.

Table 161. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Oracle

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbSysPassword	Password
-dbSysUserId	System administrator user name
-dbUserId	Common database user name
-ceiInstancePrefix **Note:** Deprecated in 6.2 for all databases except Informix, Oracle, Microsoft SQL Server.	N/A (command-line only)

Table 161. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Oracle (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files You must install the `ojdbc6.jar` driver to access the Oracle database. **Note:** Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle web site.
-dbLocation (required only if -dbDelayConfig is set to true)	Directory of database server installation
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On Informix Dynamic Server

Table 113 on page 298 shows the manageprofiles parameters available to configure the Common Event Infrastructure database used by a stand-alone server profile on Informix Dynamic Server.

Table 162. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Informix Dynamic Server

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-dbLocation (required only if **-dbDelayConfig** is set to false)	Directory of database server installation
-ceiDbName	Common Event Infrastructure database name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product
-dbInstance	Instance name
-dbUserId	User name to authenticate with the database

Table 162. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Informix Dynamic Server (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-ceiInstancePrefix **Note:** Deprecated in 6.2 for all databases except Informix, Oracle, Microsoft SQL Server.	N/A (command-line only)
-dbJDBCClasspath	Location (directory) of JDBC driver classpath files
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
N/A	Override the destination directory for generated scripts

On Microsoft SQL Server

Table 114 on page 299 shows the manageprofiles parameters that are available to configure the Common database that is used by a stand-alone server, deployment manager, or custom profile on Microsoft SQL Server. Three JDBC drivers are available for this database: DataDirect Connect JDBC (XA) 3.5 build 37 (type 4), IBM WebSphere embedded Connect JDBC (XA) 3.5 build 37 (type 4), and Microsoft SQL Server JDBC Driver, version 1.2. The driver names that are displayed on the Database Configuration page are Microsoft SQL Server (DataDirect) and Microsoft SQL Server (Microsoft).

Note: Support for the Microsoft SQL Server JDBC Driver, version 1.2 was added in WebSphere Process Server, version 6.2.0.1.

Table 163. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Microsoft SQL Server.

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbDelayConfig	Delay execution of database scripts (must select if using a remote database)
-dbHostName	Database server host name (for example IP address)
-ceiDbInstallDir (required only if **-dbDelayConfig** is set to true)	N/A (command-line only)
-ceiDbName	Common Event Infrastructure database name
-dbUserId	Common database user name
-dbPassword	Password for database authentication
-dbServerPort	Server port
-dbType	Choose a database product

Table 163. Available manageprofiles parameters for configuration of Common Event Infrastructure database using Microsoft SQL Server. (continued)

Parameter	Related field on Database Configuration pages in Profile Management Tool
-dbInstance (required only if **-dbDelayConfig** is set to true)	Instance name
-ceiDbUser **Note:** This user must be different from the **dbUserId**. **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	CEI database user name
-ceiDbPassword **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	CEI database password
-ceiInstancePrefix **Note:** Deprecated in 6.2 for all databases except Informix, Oracle, Microsoft SQL Server.	N/A (command-line only)
-dbOutputScriptDir	Database script output directory **Note:** Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.
-ceiOverrideDataSource	N/A (command-line only)
-ceiSaPassword **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	Admin user password
-ceiSaUser **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.	Admin user name
N/A	Override the destination directory for generated scripts

manageprofiles command-line utility

The manageprofiles command-line utility creates a profile, which is the set of files that define the runtime environment for a deployment manager, a managed node, or a stand-alone server.

The profile defines the runtime environment and includes all of the files that the server processes can change during runtime.

The manageprofiles command-line utility and its graphical user interface, the Profile Management Tool, are the only ways to create profiles, or the only ways to create runtime environments. You can also augment profiles and delete profiles with the manageprofiles command-line utility.

The command file is located in the *install_root*/bin directory. The command file is a script named manageprofiles.sh for Linux and UNIX platforms or manageprofiles.bat for Windows platforms.

The manageprofiles command-line utility creates a log for every profile that it creates, deletes, or augments. The logs are in the following directory, depending on platform:

- [Linux] [UNIX] *install_root*/logs/manageprofiles

- [Windows] *install_root*\logs\manageprofiles

The files are named as follows:
- *profile_name*_create.log
- *profile_name*_augment.log
- *profile_name*_delete.log

Templates for each profile are located in the *install_root*/profileTemplates directory. Within this directory are various directories that correspond to different profile types. The directories are the paths that you indicate while using the manageprofiles command-line utility with the **-templatePath** option. You can also specify profile templates that lie outside the installation root if they exist. Use the following templates with WebSphere Process Server:
- default.wbiserver: for a WebSphere Process Server stand-alone server profile, which defines a stand-alone server.
- dmgr.wbiserver: for a WebSphere Process Server deployment manager profile, which defines a deployment manager.
- managed.wbiserver: for a WebSphere Process Server custom profile, which, when federated to a deployment manager, defines a managed node.
- default.esbserver: for a WebSphere Enterprise Service Bus stand-alone server profile, which defines a stand-alone server.
- dmgr.esbserver: for a WebSphere Enterprise Service Bus deployment manager profile, which defines a deployment manager.
- managed.esbserver: for a WebSphere Enterprise Service Bus custom profile, which, when federated to a deployment manager, defines a managed node.

Syntax

The manageprofiles command-line utility is used to perform the following tasks:
- Creating a profile (**-create** parameter).

  Follow the instructions in "Creating profiles using the manageprofiles command-line utility" on page 253.
- Augmenting a profile (**-augment** parameter).

  Follow the instructions in "Augmenting profiles using the manageprofiles command-line utility" on page 340.

  Note: Using profiles that have been unaugmented (**-unaugment** parameter) is not supported.
- Deleting a profile (**-delete** parameter).

  Follow the instructions in "Deleting profiles using the manageprofiles command-line utility" on page 403.
- Deleting all profiles (**-deleteAll** parameter)
- Listing all profiles (**-listProfiles** parameter)
- Getting the name of an existing profile from its name (**-getName** parameter)
- Getting the name of an existing profile from its path (**-getPath** parameter)
- Validating a profile registry (**-validateRegistry** parameter)

- Validating and updating a profile registry (**-validateAndUpdateRegistry** parameter)
- Getting the default profile name (**-getDefaultName** parameter)
- Setting the default profile name (**-setDefaultName** parameter)
- Backing up a profile (**-backupProfile** parameter)
- Restoring a profile (**-restoreProfile** parameter)
- Using a response file containing the information required to run a manageprofiles command-line utility (**-response** parameter)

For detailed help including the required parameters for each of the tasks accomplished with the manageprofiles command-line utility, use the **-help** parameter. The following is an example of using the help parameter with the manageprofiles command-line utility **-augment** parameter on Windows operating systems: `manageprofiles.bat -augment -help`. The output specifies which parameters are required and which are optional.

Parameters

Depending on the operation that you want to perform with the manageprofiles command-line utility, you might need to provide one or more of the parameters described in "manageprofiles parameters." The Profile Management Tool validates that the required parameters are provided and the values entered for those parameters are valid. Be sure to type the name of the parameters with the correct case, because the command line does not validate the case of the parameter name. Incorrect results can occur when the parameter case is not typed correctly.

Command output

On completion, the command displays a statement similar to one of the following messages. (Exact wording varies depending on whether you created, deleted or augmented a profile.)
- `INSTCONFSUCCESS: Profile creation succeeded.`
- `INSTCONFFAILED: Profile creation failed.`
- `INSTCONFPARTIALSUCCESS: Some non-critical post installation configuration actions did not succeed.`

In some cases, the statement is displayed more than once. For example, the INSTCONFSUCCESS line is displayed three times at the command line. For more information, see Installation and profile creation log files

manageprofiles parameters
Use the following parameters with the manageprofiles command-line utility for WebSphere Process Server.

The manageprofiles command file is located in the *install_root*/bin directory. The command file is a script named `manageprofiles.sh` for Linux and UNIX platforms, or `manageprofiles.bat` for Windows platforms.

Before you begin using the manageprofiles command-line utility, make sure that you understand all prerequisites for creating and augmenting profiles. For more information about prerequisites, see "Prerequisites for creating or augmenting profiles" on page 189. For more information about creating and augmenting profiles, see "Creating profiles using the manageprofiles command-line utility" on page 253 and "Augmenting profiles using the manageprofiles command-line utility" on page 340.

Attention: When creating a WebSphere Process Server profile, use only the parameters that are documented in the information center for WebSphere Process Server.

Note: All parameters are case-sensitive.

The following options are available for the manageprofiles command-line utility:

-adminUserName *adminUser_ID*
> Specifies the user ID that is used for administrative security. For augmenting an existing profile that has administrative security enabled, this parameter is required.

-adminPassword *adminPassword*
> Specifies the password for the administrative security user ID specified with the `-adminUserName` parameter. For augmenting an existing profile that has administrative security enabled, this parameter is required.

-appSchedulerServerName
> The name of the server where the WebSphere Process Server Application Scheduler is configured to run. This parameter is valid for profile augmentation when the profile has multiple servers defined.

-augment
> Use the augment parameter to make changes to an existing profile with an augmentation template. The augment parameter causes the manageprofiles command-line utility to update or augment the profile identified in the **-profileName** parameter using the template in the **-templatePath** parameter. The augmentation templates that you can use are determined by which IBM products and versions are installed in your environment.

> **Note:** Do not manually modify the files that are located in the *install_dir*/profileTemplates directory. For example, if you are changing the ports during profile creation, use the Profile Management Tool or the -startingPort or -portsFile arguments on the manageprofiles command-line utility instead of modifying the file in the profile template directory.

> Specify the fully qualified file path for **-templatePath**. For example:

> ```
> manageprofiles(.bat)(.sh) -augment -profileName profile_name
>  -templatePath fully_qualified_template_path
> ```

-backupProfile
> Performs a file system back up of a profile folder and the profile metadata from the profile registry file.

> This parameter is not supported with WebSphere Process Server.

-backupFile *backupFile_name*
> Backs up the profile registry file to the specified file. You must provide a fully qualified file path for the *backupFile_name*.

-cbeServerName
> The name of the server where the WebSphere Process Server Common Base Event Browser is configured to run.

-cdbSchemaName
> The database schema name. This parameter is valid for all database types except for Oracle, Informix, Microsoft SQL Server (DataDirect), and Microsoft SQL Server. It is not used for DB2 for z/OS v8, DB2 for z/OS v9, and DB2 UDB for iSeries (Toolbox) if dbSchemaName is set. Table 164 on page 379 lists the default schema names.

Table 164. Default schema names

Database	Default schema name
Derby Embedded or Derby Embedded 40	APP
Derby Network Server or Derby Network Server 40	dbUserId
DB2 Universal	dbUserId
DB2 for z/OS v8, DB2 for z/OS v9	dbUserId
DB2 UDB for iSeries (Toolbox)	dbUserId

> **Note:** Note: You can specify a different schema for supported databases, but the recovery tables are always created using the default schema name for Derby Embedded or Derby Embedded 40, Derby Network Server or Derby Network Server 40, and DB2 Universal.

-ceiBufferPool4k
> Specifies the name of the 4K buffer pool for the Common Event Infrastructure. This buffer pool must be active before the database DDL scripts can be run.
>
> **Note:** Deprecated in 6.2 for all databases except DB2 for z/OS.

-ceiBufferPool8k
> Specifies the name of the 8K buffer pool for the Common Event Infrastructure. This buffer pool must be active before the database DDL scripts can be run.
>
> **Note:** Deprecated in 6.2 for all databases except DB2 for z/OS.

-ceiBufferPool16k
> Specifies the name of the 16K buffer pool for the Common Event Infrastructure. This buffer pool must be active before the database DDL scripts can be run.
>
> **Note:** Deprecated in 6.2 for all databases except DB2 for z/OS.

-ceiDbInstallDir
> The directory where the database is installed for the Common Event Infrastructure. This parameter is required only if you specified true for the dbDelayConfig parameter.

-ceiDbName
> The name of the Common Event Infrastructure event database to be created. For DB2 databases, Derby databases, Informix databases, and Microsoft SQL Server databases, the default value is event if not specified. For DB2 for IBM i (DB2 for i5/OS) Toolbox databases, the default value is *SYSBAS if not specified.
>
> For Oracle databases, the Oracle System Identifier (SID) must have been already created and available for the event service command to create the tables and populate the tables with data. The default value is orcl if not specified.

-ceiDbNodeName
> The DB2 node name (must be 8 characters or less) for the Common Event Infrastructure. This node must be already cataloged and configured to communicate with the DB2 server. This parameter must be set if the current workstation is configured as a DB2 client and the parameter **dbDelayConfig** is set to true.

Note: Deprecated in 6.2 for all databases except DB2 client.

-ceiDbUser

Note: Deprecated in 6.2 for all databases except Microsoft SQL Server. Specifies the user ID to use for the Common Event Infrastructure event database.

For DB2 databases, the default value is `db2inst1` if not specified. For DB2 for z/OS databases, it specifies the user ID that has privileges to create and drop the databases. This parameter is required.

For DB2 for IBM i (DB2 for i5/OS) Toolbox databases, it specifies the user ID that has privileges to create and drop the databases. This parameter is required.

For Derby databases, it is the user ID used by the data source for the Derby database authentication. This parameter is optional when the WebSphere domain security is disabled and is required when the WebSphere domain security is enabled.

For Informix databases, it specifies the Informix database schema user ID that will own the event service database tables. The WebSphere data source uses this user ID to authenticate the Informix database connection. This parameter is required.

For Oracle databases, it specifies the Oracle schema user ID that will own the event service Oracle tables. The user ID will be created during the database creation and the WebSphere data source uses this user ID to authenticate the Oracle database connection. The default value is `ceiuser` if not specified.

For Microsoft SQL Server databases, it specifies the SQL Server user ID that will own the event service tables. The default value is `ceiuser` if not specified.

-ceiDiskSizeInMB
The database size in MB to be created for the Common Event Infrastructure event database. The lowest value that can be set is 10 MB. For DB2 for z/OS, the default value is 100 MB if not specified.

Note: Deprecated in 6.2 for all databases except DB2 for z/OS.

-ceiInstancePrefix
For Informix, Oracle, and Microsoft SQL Server databases, the command uses the Common Event Infrastructure event database instance name to group the database files in a directory with unique names. The default value is `ceiinst1` if not specified.

Note: Deprecated in 6.2 for all databases except Informix, Oracle, Microsoft SQL Server.

-ceiOverrideDataSource
When this parameter is set to true, the command removes any existing Common Event Infrastructure service data source at the specified scope before creating a new one. When this parameter is set to false, the command does not create an event service data source at the specified scope if another event service data source is found at the same scope. The default value is false if not specified.

-ceiSaUser
The Microsoft SQL Server ID that has privileges to create tables, devices, and

caches for the Common Event Infrastructure. This parameter is required if the **dbDelayConfig** parameter is set to true.

Note: Deprecated in 6.2 for all databases except Microsoft SQL Server.

-ceiSaPassword
> The password for the Microsoft SQL Server ID that has privileges to create tables, devices, and caches for the Common Event Infrastructure. This parameter is required if you specify a value for the **ceiSaUser** parameter, unless the sa user ID does not have a password.

> **Note:** Deprecated in 6.2 for all databases except Microsoft SQL Server.

-cellName *cell_name*
> Specifies the cell name of the profile for the Common Event Infrastructure. Use a unique cell name for each profile. This parameter is for profile creation only. Do not supply this parameter when augmenting an existing profile.

> The default value for this parameter is based on a combination of the short host name, the constant `Cell`, and a trailing number, for example:

```
if (DMgr)
 shortHostNameCellCellNumber
else
 shortHostNameNodeNodeNumberCell
```

> where *CellNumber* is a sequential number starting at `01` and *NodeNumber* is the node number that you used to define the node name.

> The value for this parameter must not contain spaces or any characters that are not valid such as the following: `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\`, and `|`.

-configureBPC `true | false`
> Determines whether the Business Process Choreographer sample configuration is created. If you set this parameter to `true`, the **-adminUserName** and **-adminPassword** parameters also must be set. In addition, if this parameter is set to `true`, the **dbCommonForME** and **fileStoreForME** parameter values are used. For example, the Business Process Choreographer messaging engine will either create its tables in the common database, or use the file store. For more information, see Planning the topology, setup, and configuration path. The default for this parameter is the same value as the **-enableAdminSecurity** parameter.

> **Note:** The Business Process Choreographer sample configuration does not use the common database (WPRCSDB). It always uses a Derby database, which is not supported in a network deployment environment. If you plan to federate this stand-alone profile later, do not set **-configureBPC** to `true`.

> **Note:** If you plan to use a database other than Derby, or you plan to federate this stand-alone server later, set **-configureBPC** to `false`.

-configureBRM `true | false`
> Configures the business rules manager. The default value is `false`.

-configureBSpace `true | false`
> Configures Business Space powered by WebSphere, which provides an integrated user experience for application users across the IBM Websphere Business Process Management portfolio. The default value is `true`. Business Space is supported with the following database products: Derby Embedded or Derby Embedded 40, Derby Network Server or Derby Network Server 40, DB2

Universal, DB2 Data Server, DB2 for IBM i (DB2 for i5/OS), DB2 for z/OS, Oracle, and Microsoft SQL Server 2005 and 2008.

Important: If the Common database you use for WebSphere Process Server does not match the supported databases for Business Space, the manageprofiles command-line utility uses a Derby Embedded or Derby Embedded 40 database for the Business Space configuration. You cannot federate this profile into a deployment environment later, because Derby Embedded or Derby Embedded 40 is not supported for deployment environments.
For more information about configuring Business Space for deployment environments, see Configuring Business Space under Related information.

-create
Creates the profile.

Specify manageprofiles -create -templatePath *fully_qualified_file_path_to_template* -help for specific information about creating a profile. Available templates include:

- default.wbiserver: for a WebSphere Process Server stand-alone server profile, which defines a stand-alone server.
- dmgr.wbiserver: for a WebSphere Process Server deployment manager profile, which defines a deployment manager.
- managed.wbiserver: for a WebSphere Process Server custom profile, which, when federated to a deployment manager, defines a managed node.
- default.esbserver: for a WebSphere Enterprise Service Bus stand-alone server profile, which defines a stand-alone server.
- dmgr.esbserver: for a WebSphere Enterprise Service Bus deployment manager profile, which defines a deployment manager.
- managed.esbserver: for a WebSphere Enterprise Service Bus custom profile, which, when federated to a deployment manager, defines a managed node.

-dbAppMePassword *app_me_pwd*
This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified ORACLE for **dbType**. Default is dbPassword.

-dbAppMeUserId *app_me_userID*
This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified ORACLE for **dbType**. Default user name is the first three characters of the Oracle Database name [SID]. For example: If SID is ORCL, dbAppMeUserId is ORCSA00.

-dbBPCMePassword *bpc_me_pwd*
Password for the user ID specified for **-dbBPCMeUserID**.

-dbBPCMeUserID *bpc_me_userID*
This parameter is used when the following conditions are met:

1. **dbType** = ORACLE
2. **dbCommonForME** = true
3. **configueBPC** = true

   Note: configueBPC = true is only valid for standalone profiles.

There are four possible scenarios based on how the above conditions are set:

- If any of the above three conditions is not met, the **-dbBPCMeUserID** parameter is not required. For example, if either **dbType** is not set to ORACLE, or **dbCommonForME** is not set to true, or **configueBPC** is not set to true, **-dbBPCMeUserID** will be ignored.
- If all three conditions are met, and both the **-dbBPCMeUserID** and **-dbBPCMePassword** parameters are set, then they are used for the Oracle Business Process Choreographer messaging engine authentication alias. In addition, **-dbBPCMeUserID** is used for the Oracle Business Process Choreographer messaging engine schema name.
- If all three conditions are met, but only one of the **-dbBPCMeUserID** and **-dbBPCMePassword** parameters is set is set, an error will be generated.
- If all three conditions are met, and neither of the **-dbBPCMeUserID** and **-dbBPCMePassword** parameters is set, then **dbSysMePassword** must be set and is used for the Oracle Business Process Choreographer messaging engine authentication alias. A value for the Oracle Business Process Choreographer messaging engine schema name will automatically be generated and also be used for the Business Process Choreographer messaging engine authentication alias.
  - If the **dbUserId** parameter is set, its value is used for both the Oracle Business Process Choreographer messaging engine authentication alias and the Oracle Business Process Choreographer messaging engine schema name.
  - If the **dbUserId** parameter is not set, a value will be automatically generated for it.

-dbCeiMePassword *cei_me_pwd*
> This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified ORACLE for **dbType**. Default is dbPassword.

-dbCeiMeUserID *cei_me_userID*
> This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified ORACLE for **dbType**. Default user name is the first three characters of the Oracle Database name [SID]. For example: If SID is ORCL, dbCeiMeUserID is ORCCM00.

-dbCeiPassword *cei_db_pwd*
> This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified ORACLE for **dbType**. Default is dbPassword.

-dbCeiUserId *cei_userID*
> For Oracle databases, specifies the CEI user ID. This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified ORACLE for **dbType**. Default user name is the first three characters of the Oracle Database name [SID]. For example: If SID is ORCL, dbCeiUserId is ORCCEID.

-dbCommonForME
> Indicates whether to use the Common database for messaging engines. For DB2 for z/OS databases, the default value is true. For all other databases, the default value is false. If this parameter is set to false, the messaging engines will use a Derby database as default data store.

-dbCommonPassword
> This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified ORACLE for **dbType**. Default is dbPassword.

-dbCommonUserId

This parameter is needed if you enter a user-specified a user name and password during profile creation. Default user name is the first three characters of the Oracle Database name [SID]. For example: If SID is `ORCL`, dbCommonUserId is `ORCCOMM`.

-dbConnectionLocation

The location of DB2 for z/OS database.

-dbCreateNew

Indicates if you will create or reuse a database. Valid values are `true` or `false`. Default value is `true`.

-dbDelayConfig

Indicates if you will postpone table creation until after the profile is created. Valid values are `true` or `false`. The parameter is set to `false` by default. Set this parameter to `true` to delay execution of database scripts if using a remote database.

-dbDriverType

The database driver type. For Oracle databases, valid values are `ORACLE_THIN` or `ORACLE_OCI`. For DB2 databases, valid values are 2 or 4.

-dbHostName

The database server host name or IP address. The default value is `localhost`.

-dbInstance

The database instance name for Informix databases.

-dbJDBCClasspath

The location of JDBC driver files. You must install the `ojdbc6.jar` driver to access the Oracle database.

Note: Oracle 10g does not contain the `ojdbc6.jar` driver. You can download it from the Oracle web site.

-dbLocation

The directory of the ORACLE_HOME or Database installation directory if you are using Oracle or Informix databases. This parameter is required when the parameter **dbDelayConfig** is set to `false`.

-dbName

The name of the database. By default, the value is set to `orcl` for Oracle databases, to `*SYSBAS` for IBM i databases, and to `WPRCSDB` for all other supported databases.

-dbOutputScriptDir

The location for exported database scripts.

Note: Only available if **Override the destination directory for generated scripts** option is selected. The value must be an absolute path. If you set a relative path, the SQL scripts will not be exported or executed, which will result in numerous exceptions during server startup.

-dbPassword

The password required for database authentication. This parameter is required for all databases except Derby Embedded or Derby Embedded 40.

-dbProviderType *provider*

An optional parameter that specifies the provider type for the current dbType. Currently only applicable to the Informix dbType.

-dbSchemaName

The database schema name for DB2 for z/OS v8, DB2 for z/OS v9, and DB2 UDB for iSeries (Toolbox). If both dbSchemaName and cdbSchemaName are set, cdbSchemaName take precedence. This parameter has been deprecated in WebSphere Process Server V7.

-dbServerPort

The database server port number. Depending on the database you are using, you can specify a different port number instead of the default port number.

-dbStorageGroup

The storage group name for DB2 z/OS databases.

-dbSysMePassword *sys_me_pwd*

This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified `ORACLE` for **dbType**. Default is `dbPassword`.

-dbSysMeUserID *sys_me_userID*

This parameter is needed if you enter a user-specified a user name and password during profile creation and if you specified `ORACLE` for **dbType**. Default user name is the first three characters of the Oracle Database name [SID]. For example: If SID is `ORCL`, dbSysMeUserID is `ORCSS00`.

-dbSysPassword *sys_pwd*

This parameter is required when **dbDelayConfig** is set to `false` and if you specified `ORACLE` for **dbType**.

-dbSysUserId *sys_user_id*

This ID must have SYSDBA privileges. Do not use the Oracle internal user `sys`. This parameter is required when **dbDelayConfig** is set to `false` and if you specified `ORACLE` for **dbType**.

-dbType

The database type.

Set one of the following values for the type of database product you are using with WebSphere Process Server.

- `DERBY_EMBEDDED40` for a Derby Embedded database using a Derby Embedded 40 JDBC Provider
- `DERBY_NETWORKSERVER40` for a Derby Network Server database using a Derby Network Server 40 JDBC Provider
- `DB2_UNIVERSAL` for a DB2 Universal database
- `DB2_DATASERVER` for a DB2 Data Server database
- `DB2UDBOS390_V8_1` for a DB2 for z/OS v8 database
- `DB2UDBOS390_V9_1` for a DB2 for z/OS v9 database
- `DB2UDBISERIES_TOOLBOX` for a DB2 for IBM i or DB2 for i5/OS database using a Toolbox driver
- `INFORMIX` for an Informix Dynamic Server database
- `MSSQLSERVER_DATADIRECT` for a Microsoft SQL Server database using a DataDirect driver
- `MSSQLSERVER_MICROSOFT` for a Microsoft SQL Server database using a Microsoft driver

Note: Support for the Microsoft SQL Server JDBC Driver, version 1.2
Microsoft SQL Server (Microsoft) driver was added in WebSphere Process
Server, version 6.2.0.1.

- `ORACLE` for an Oracle database

-dbUserId

User ID for all database types. Specifies the user ID that has privileges to
create and drop the databases. The WebSphere data source uses this ID to
authenticate the database connection.

For DB2 databases, it specifies the database user ID that will own the database
tables. The default value is `db2inst1`. For DB2 for z/OS databases, it specifies
the user ID that has privileges to create and drop the databases. This
parameter is required.

For DB2 for IBM i (DB2 for i5/OS) Toolbox databases, it specifies the user ID
that has privileges to create and drop the databases. This parameter is
required.

For Derby databases, it is the user ID used by the data source for the Derby
database authentication. This applies only to the Derby Networkserver
database. Defaults to the `-adminUserName` if security enabled, otherwise to `TEST`.

For Derby Network Server databases, it specifies the Derby user ID of the user
that owns the database tables. CommonDB defaults to the adminUserName if
security enabled, otherwise to `TEST`.

For Informix databases, it specifies the Informix database user ID that will own
the database tables. The WebSphere data source uses this user ID to
authenticate the Informix database connection. This parameter is required.

For Oracle databases, it specifies the Oracle user ID that owns the database
tables. The specified user ID will be used for deployment environment profile
creation and must have SYSDBA privileges. The user ID will be created during
the database creation and the WebSphere data source uses this user ID to
authenticate the Oracle database connection. The default value is `ceiuser` if not
specified for CEI.

For Microsoft SQL Server databases, it specifies the SQL Server user ID that
will own the database tables.

-debug

Turns on the debug function of the Apache Ant utility, which the
manageprofiles command-line utility uses.

-defaultPorts

Assigns the default or base port values to the profile.

Do not use this parameter when using the `-startingPort` or `-portsFile`
parameter.

During profile creation, the manageprofiles command-line utility uses an
automatically generated set of recommended ports if you do not specify the
`-startingPort` parameter, the `-defaultPorts` parameter or the `-portsFile`
parameter. The recommended port values can be different than the default port
values based on the availability of the default ports.

Note: Do not use this parameter if you are using the managed profile
template.

-delete

Deletes the profile.

Deleting a profile does not delete the profile directory. For example, if you create a profile in the /usr/WebSphere/ProcServer/profiles/managedProfile directory, the directory remains after you delete the profile.

You can delete or leave the directory. However, the *profile_root*/logs directory contains information about uninstalling the profile. For example, you might retain the _nodeuninst.log file to determine the cause of any problem during the uninstallation procedure.

If you delete a profile that has augmenting templates registered to it in the profile registry, then unaugment actions are performed automatically.

-deleteAll

Deletes all registered profiles.

Deleting a profile does not delete the profile directory. For example, suppose that you create a profile in the /usr/WebSphere/ProcServer/profiles/managedProfile directory, the directory remains after you delete the profile.

You can delete or leave the directory. However, the *profile_root*/logs directory contains information about uninstalling the profile. For example, you might retain the _nodeuninst.log file to determine the cause of any problem during the uninstallation procedure.

If you delete a profile that has augmenting templates registered to it in the profile registry, then unaugment actions are performed automatically.

-dmgrHost *dmgr_host_name*

Identifies the workstation where the deployment manager is running. Specify this parameter and the **dmgrPort** parameter to federate a custom profile as it is created or augmented. This parameter is available with the managed.wbiserver and managed.esbserver profile templates.

The host name can be the long or short DNS name or the IP address of the deployment manager workstation.

Specifying this optional parameter directs the manageprofiles command-line utility to attempt to federate the custom node into the deployment manager cell as it creates the custom profile. This parameter is ignored when creating a deployment manager profile or stand-alone server profile.

If you federate a custom node when the deployment manager is not running, the installation indicator in the logs is INSTCONFFAILED to indicate a complete failure. The resulting custom profile is unusable. You must move the custom profile directory out of the profile repository (the profile's installation root directory) before creating another custom profile with the same profile name.

If you have enabled security or changed the default JMX connector type, you cannot federate with the manageprofiles command-line utility. Use the addNode command instead.

The default value for this parameter is localhost. The value for this parameter must be a properly formed host name and must not contain spaces or characters that are not valid such as the following: *, ?, ", <, >, , , /, \, and |. A connection to the deployment manager must also be available in conjunction with the dmgrPort parameter.

-dmgrPort *dmgr_port_number*

Identifies the SOAP port of the deployment manager. Specify this parameter and the **dmgrHost** parameter to federate a custom profile as it is created or augmented. The deployment manager must be running and accessible.

If you have enabled security or changed the default JMX connector type, you cannot federate with the manageprofiles command-line utility. Use the addNode command instead.

The default value for this parameter is 8879. The port that you indicate must be a positive integer and a connection to the deployment manager must be available in conjunction with the `dmgrHost` parameter.

-enableAdminSecurity `true` | `false`

Enables administrative security. Valid values include `true` or `false`. The default value is `false`. If you are creating profiles for a deployment environment, you must set this parameter to `true`. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

When enableAdminSecurity is set to `true`, you must also specify the parameters `-adminUserName` and `-adminPassword` along with the values for these parameters. If samples were installed during the application server installation, you must also specify the `-samplesPassword` parameter when creating a profile for which administrative security is enabled. If the `-samplesPassword` parameter is not specified when administrative security is enabled, the profile is created successfully, but when you attempt to run the samples, exceptions and failures will be put in the server system out log.

Note: If you set **enableAdminSecurity** to true, then **configureBPC** will also default to `true`. Check the description of the **configureBPC** parameter if you explicitly need to set it to `false` for your intended setup.

Linux **-enableService `true` | `false`**

Enables the creation of a Linux service. Valid values include `true` or `false`. The default value for this parameter is `false`. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

When the manageprofiles command-line utility is run with the `-enableService` option set to `true` , the Linux service is created with the profile when the command is run by the root user. When a nonroot user runs the manageprofiles command-line utility, the profile is created, but the Linux service is not. The Linux service is not created because the nonroot user does not have sufficient permission to set up the service. An `INSTCONPARTIALSUCCESS` result is displayed at the end of the profile creation and the profile creation log *install_root*/logs/manageprofiles/*profile_name*_create.log contains a message indicating the current user does not have sufficient permission to set up the Linux service.

-federateLater `true` | `false`

Indicates if the managed profile will be federated during profile creation or if you will federate it later using the addNode command. If you are creating a WebSphere Process Server profile, do not supply a value; use the default of `true`.

-federateLaterProcServer `true` | `false`

Indicates if the managed profile will be federated later using the managed.wbiserver template. Valid values are `true` or `false`. If the **dmgrHost**, **dmgrPort**, **dmgrAdminUserName** and **dmgrAdminPassword** parameters are not set, the default value for this parameter is `true`.

-federateLaterWESB `true` | `false`

Indicates if the managed profile will be federated later using the managed.wesbserver template. Valid values are `true` or `false`. If the **dmgrHost**,

dmgrPort, **dmgrAdminUserName** and **dmgrAdminPassword** parameters are not set, the default value for this parameter is `true`.

-fileStoreForME `true` | `false`

If set to true, the file store data store will be used for the messaging engines. The default value for this parameter is `false`.

Note: The **-dbCommonForME** and **-fileStoreForME** parameters cannot both be set to `true`. This causes a validation error.

-getDefaultName

Returns the name of the default profile.

-getName

Gets the name for a profile registered at a given `-profilePath` parameter.

-getPath

Gets the file system location for a profile of a given name. Requires the `–profileName` parameter.

-help

Displays command syntax.

-hostName *host_name*

Specifies the host name where you are creating the profile. Do not supply this parameter when augmenting an existing profile. This should match the host name that you specified during installation of the initial product. The default value for this parameter is the long form of the domain name system. This parameter is required for profile creation only. The value for this parameter must be a valid IPv6 host name and must not contain spaces or any characters that are not valid such as the following: `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\`, and `|`.

-ignoreStack

An optional parameter that is used with the -templatePath parameter to unaugment a particular profile that has been augmented.

Note: Using profiles that have been unaugmented (**-unaugment** parameter) is not supported.

-importPersonalCertKS *keystore_path*

Specifies the path to the keystore file that you use to import a personal certificate when you create the profile. The personal certificate is the default personal certificate of the server.

When you import a personal certificate as the default personal certificate, import the root certificate that signed the personal certificate. Otherwise, the manageprofiles utility adds the public key of the personal certificate to the trust.p12 file and creates a root signing certificate.

The `-importPersonalCertKS` parameter is mutually exclusive with the `-personalCertDN` parameter. If you do not specifically create or import a personal certificate, one is created by default.

When you specify any of the parameters that begin with -importPersonal, you must specify them all.

-importPersonalCertKSType *keystore_type*

Specifies the type of the keystore file that you specify on the `-importPersonalCertKS` parameter. Values might be JCEKS, CMSKS, PKCS12, PKCS11, and JKS. However, this list can change based on the provider in the java.security file.

When you specify any of the parameters that begin with -importPersonal, you must specify them all.

-importPersonalCertKSPassword *keystore_password*
Specifies the password of the keystore file that you specify on the `-importPersonalCertKS` parameter.

When you specify any of the parameters that begin with -importPersonal, you must specify them all.

-importPersonalCertKSAlias *keystore_alias*
Specifies the alias of the certificate that is in the keystore file that you specify on the `-importPersonalCertKS` parameter. The certificate is added to the server default keystore file and is used as the server default personal certificate.

When you specify any of the parameters that begin with -importPersonal, you must specify them all.

-importSigningCertKS *keystore_path*
Specifies the path to the keystore file that you use to import a root certificate when you create the profile. The root certificate is the certificate that you use as the server default root certificate. The `-importSigningCertKS` parameter is mutually exclusive with the `-signingCertDN` parameter. If you do not specifically create or import a root signing certificate, one is created by default.

When you specify any of the parameters that begin with -importSigning, you must specify them all.

-importSigningCertKSType *keystore_path*
Specifies the type of the keystore file that you specify on the `-importSigningCertKS` parameter. Valid values might be JCEKS, CMSKS, PKCS12, PKCS11, and JKS. However, this list can change based on the provider in the java.security file.

When you specify any of the parameters that begin with -importSigning, you must specify them all.

-importSigningCertKSPassword *keystore_password*
Specifies the password of the keystore file that you specify on the `-importSigningCertKS` parameter.

When you specify any of the parameters that begin with -importSigning, you must specify them all.

-importSigningCertKSAlias *keystore_alias*
Specifies the alias of the certificate that is in the keystore file that you specify on the `-importSigningCertKS` parameter. The certificate is added to the server default root keystore and is used as the server default root certificate.

When you specify any of the parameters that begin with -importSigning, you must specify them all.

-isDefault
Specifies that the profile identified by the accompanying `-profileName` parameter is to be the default profile once it is registered. When issuing commands that address the default profile, it is not necessary to use the `-profileName` attribute of the command.

-isDeveloperServer
Specifies whether the server is intended for development purposes only. This parameter is useful when creating profiles to test applications on a

non-production server prior to deploying the applications on their production application servers. This parameter is valid only for creating profiles on WebSphere Process Server.

If **-isDeveloperServer** is set when creating a WebSphere Process Server profile, then a preconfigured VMM file repository is installed. This file repository contains a sample organization that can be used to test Business Process Choreographer people resolution, ready for you to use as is.

-keyStorePassword *keyStore_password*
> Specifies the password to use on all keystore files created during profile creation. Keystore files are created for the default personal certificate and the root signing certificate.

-listAugments
> Lists the registered augments on a profile that is in the profile registry. You must specify the `-profileName` parameter with the `-listAugments` parameter.

-listProfiles
> Lists all defined profiles.

-ndtopology
> Indicates if you want to use the deployment environment path for creating the profile. Valid values are `true` or `false`.

-nodeName *node_name*
> Specifies the node name for the node that is created with the new profile. Do not supply this parameter when augmenting an existing profile. Use a unique value within the cell or on the workstation. Each profile that shares the same set of product binaries must have a unique node name. This parameter is required for profile creation only with the default.wbiserver, dmgr.wbiserver, and managed.wbiserver templates.

> `Linux` `UNIX` `Windows` The default value for this parameter is based on the short host name, profile type, and a trailing number, for example:

```
if (DMgr)
 shortHostNameCellManagerNodeNumber
else
 shortHostNameNodeNodeNumber
```

> where *NodeNumber* is a sequential number starting at `01`.

> The value for this parameter must not contain spaces or any characters that are not valid such as the following: *, ?, ", <, >, ,, /, \, and |, .

-omitAction *feature1 feature2... featureN*
> An optional parameter that excludes profile features.

> Each profile template comes predefined with certain optional features. The `samplesInstallAndConfig` option is only available when the product is installed with samples applications selected. The following optional features can be used with the `-omitAction` parameter for the following profile templates:

> * **default** - Application server
>   - deployAdminConsole
>   - samplesInstallAndConfig
>   - defaultAppDeployAndConfig
> * **dmgr** - Deployment manager
>   - deployAdminConsole

-personalCertDN *distinguished_name*

Specifies the distinguished name of the personal certificate that you are creating when you create the profile. Specify the distinguished name in quotation marks. This default personal certificate is located in the server keystore file. The `-importPersonalCertKSType` parameter is mutually exclusive with the `-personalCertDN` parameter. See the `-personalCertValidityPeriod` parameter and the `-keyStorePassword` parameter.

-personalCertValidityPeriod *validity_period*

An optional parameter that specifies the amount of time in years that the default personal certificate is valid. If you do not specify this parameter with the `-personalCertDN` parameter, the default personal certificate is valid for one year.

-portsFile *file_path*

An optional parameter that specifies the path to a file that defines port settings for the new profile. Do not supply this parameter when augmenting an existing profile.

Do not use this parameter when using the `-startingPort` or `-defaultPorts` parameter.

During profile creation, the manageprofiles command-line utility uses an automatically generated set of recommended ports if you do not specify the `-startingPort` parameter, the `-defaultPorts` parameter or the `-portsFile` parameter. The recommended port values can be different than the default port values based on the availability of the default ports.

-profileName *profile_name*

Specifies the name of the profile. Use a unique value when creating a profile.

Each profile that shares the same set of product binaries must have a unique name. The default profile name is based on the profile type and a trailing number, for example:

`profileType ProfileNumber`

where *profileType* is a value such as `ProcSrv`, `Dmgr`, or `Custom` and *ProfileNumber* is a sequential number that creates a unique profile name.
The value for this parameter must not contain spaces or characters that are not valid such as the following: `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\`, and `|`. The profile name that you choose must not be in use.

-profilePath *profile_root*

Specifies the fully qualified path to the profile, which is referred to throughout the information center as the *profile_root*.

For example:

`-profilePath profile_root`

Use this parameter when creating profiles only. Do not set this parameter for augmenting an existing profile.

▭Windows▭ **On Windows platforms:** If the fully qualified path contains spaces, enclose the value in quotation marks.

The default value is based on the *install_root* directory, the profiles subdirectory, and the name of the file.

For example, the default for profile creation is:

`WS_WSPROFILE_DEFAULT_PROFILE_HOME/profileName`

where *WS_WSPROFILE_DEFAULT_PROFILE_HOME* is defined in the `wasprofile.properties` file in the *install_root*`/properties` directory.

The value for this parameter must be a valid path for the target system and must not be currently in use.

You must have permissions to write to the directory.

-response *response_file*
Accesses all API functions from the command line using the manageprofiles command-line utility.

The command line interface can be driven by a response file that contains the input arguments for a given command in the properties file in key and value format. The following is an example response file for a create operation:

```
create
profileName=testResponseFileCreate
profilePath=profile_root
templatePath=install_root/profileTemplates/default
nodeName=myNodeName
cellName=myCellName
hostName=myHostName
omitAction=myOptionalAction1, myOptionalAction2
```

Windows **On Windows platforms:** The path statement in the Windows operating system can use either forward slashes (/) or back slashes (\). If the path statement uses back slashes, then the response file requires double back slashes for the response file to correctly understand the path. Here is an example of a response file for a create operation that uses the double back slashes:

```
create
templatePath=C:\\WebSphere\\ProcServer\\profileTemplates\\default
```

To determine which input arguments are required for the various types of profile templates and action, use the manageprofiles command-line utility with the **-help** parameter.

-restoreProfile
Restores a profile backup. Must be used with the `-backupFile` parameter. This parameter is not supported for WebSphere Process Server.

-samplesPassword *samplesPassword*
Creates a password to be used for samples. The password is used to restrict access to Web application samples installed during the installation of the application server.

-serverName *server_name*
Specifies the name of the server. If you do not specify this parameter, the default server name is `server1` for the default profile.

-serverType `DMGR`
Specifies the type of management profile. Specify `DMGR` for a management profile. This parameter is required when you create a management profile.

Linux **-serviceUserName** *service_user_ID*
Specifies the user ID that is used during the creation of the Linux service so that the Linux service will run under this user ID. The Linux service runs whenever the user ID is logged on.

-setDefaultName
Sets the default profile to one of the existing profiles. Must be used with the `-profileName` parameter, for example:

Configuring **393**

```
manageprofiles(.bat)(.sh) -setDefaultName -profileName profile_name
```

-signingCertDN *distinguished_name*

Specifies the distinguished name of the root signing certificate that you create
when you create the profile. Specify the distinguished name in quotation
marks. This default personal certificate is located in the server keystore file.
The *-importSigningCertKS* parameter is mutually exclusive with the
-signingCertDN parameter. If you do not specifically create or import a root
signing certificate, one is created by default. See the *-signingCertValidityPeriod*
parameter and the *-keyStorePassword*.

-signingCertValidityPeriod *validity_period*

An optional parameter that specifies the amount of time in years that the root
signing certificate is valid. If you do not specify this parameter with the
-signingCertDN parameter, the root signing certificate is valid for 20 years.

-startingPort *startingPort*

Specifies the starting port number for generating and assigning all ports for the
profile.

Do not set this parameter if you are augmenting an existing profile. Port values
are assigned sequentially from the **-startingPort** value, omitting those ports
that are already in use. The system recognizes and resolves ports that are
currently in use and determines the port assignments to avoid port conflicts.

Do not use this parameter with the **-defaultPorts** or **-portsFile** parameters.

During profile creation, the manageprofiles command-line utility uses an
automatically generated set of recommended ports if you do not specify the
-startingPort parameter, the **-defaultPorts** parameter or the **-portsFile**
parameter. The recommended port values can be different than the default port
values based on the availability of the default ports.

Note: Do not use this parameter if you are using the managed profile
template.

-templatePath *template_path*

Specifies the directory path to the template files in the installation root
directory. Within the `profileTemplates` directory are various directories that
correspond to different profile types and that vary with the type of product
installed. The profile directories are the paths that you indicate while using the
-templatePath option. You can specify profile templates that lie outside the
installation root, if you have any.

Use absolute paths. This parameter must exist as a directory and point to a
valid template directory. Use the following templates with WebSphere Process
Server:
- `default.wbiserver`: for a WebSphere Process Server stand-alone server
  profile, which defines a stand-alone server.
- `dmgr.wbiserver`: for a WebSphere Process Server deployment manager
  profile, which defines a deployment manager.
- `managed.wbiserver`: for a WebSphere Process Server custom profile, which,
  when federated to a deployment manager, defines a managed node.
- `default.esbserver`: for a WebSphere Enterprise Service Bus stand-alone
  server profile, which defines a stand-alone server.
- `dmgr.esbserver`: for a WebSphere Enterprise Service Bus deployment
  manager profile, which defines a deployment manager.
- `managed.esbserver`: for a WebSphere Enterprise Service Bus custom profile,
  which, when federated to a deployment manager, defines a managed node.

-topologyPattern

Determines the deployment environment patterns for the deployment manager you are creating. Valid values are `CondensedSync`, `CondensedAsync` or `Reference`.

-topologyRole

Indicates the function that the profile will play in the deployment environment, when you are federating a profile that has been created. Valid values are `ADT` for a deployment target, `Messaging` for host messaging or `Support` for supporting services. You can indicate one value or more than one value, each separated by a space, for example `ADT Messaging Support` or `Messaging` or `ADT Support`.

-unaugment

Note: Using profiles that have been unaugmented (**-unaugment** parameter) is not supported.

-unaugmentAll

Unaugments all profiles that have been augmented with a specific augmentation template. The -templatePath parameter is required with the `-unaugmentAll` parameter.

When using the `-templatePath` parameter, specify the fully qualified file path for the parameter. Optionally, specify the `-unaugmentDependents` parameter with the `-unaugmentAll` parameter to unaugment all profiles that are prerequisites of the profiles that are being unaugmented.

Note: If you use this parameter when you have no profiles augmented with the profile templates, an error might be delivered.

See also the augment parameter.

-unaugmentDependents `true|false`

If set to `true`, the parameter unaugments all the augmented profiles that are prerequisites to the profiles being unaugmented with the `-unaugmentAll` parameter. The default value for this parameter is `false`.

Optionally specify the `-unaugmentDependents` parameter with the `-unaugmentAll` parameter.

-validateAndUpdateRegistry

Checks all of the profiles that are listed in the profile registry to see if the profiles are present on the file system. Removes any missing profiles from the registry. Returns a list of the missing profiles that were deleted from the registry.

-validateRegistry

Checks all of the profiles that are listed in the profile registry to see if the profiles are present on the file system. Returns a list of missing profiles.

-validatePorts

Specifies the ports should be validated to ensure they are not reserved or in use. This parameter helps you to identify ports that are not being used. If a port is determined to be in use, the profile creation stops and an error message displays. You can use this parameter at any time on the create command line. It is recommended to use this parameter with the `–portsFile` parameter.

-wbidbDesign *design_file*

Used to specify a single design file for all of the components except BPC during profile creation. You must specify the fully qualified path to the *design_file*.

Note: BPC does not use the common database (WPRCSDB). It always uses a Derby database

Note:

-webFormConfig `true | false`

Indicates if Business Space is configured to use IBM Lotus WebForm Server to work with Human Task Management widgets. The default value for this parameter is `false`. Indicate `true` to configure Business Space to use Lotus WebForm Server. Both the **webFormConfig** and **webFormInstallRoot** parameters are required to configure Lotus WebForm Server. This parameter is valid for stand-alone server profiles only.

Note: WebForm configuration using these parameters is only valid for local WebForm Server installations.

-webFormHTTP *URL*

Specifies the location of the Webform Server Translator. The default URL for the location is `http://localhost:8085/translator`. This parameter is valid only if the **-webFormConfig** parameter is set to `true`. Valid for stand-alone server profiles only.

-webFormInstallRoot *Webform_Server_install_root*

Specifies the full path where Lotus Webform Server is installed. For example, the Lotus Webform Server install root might be `C:/IBM/LotusWebForms/3.5/WebFormServer`. This parameter is valid only if the **-webFormConfig** parameter is set to `true`. Valid for stand-alone server profiles only.

-webServerCheck `true | false`

Indicates if you want to set up Web server definitions. Valid values include `true` or `false`. The default value for this parameter is `false`. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

-webServerHostname *webserver_host_name*

The host name of the server. The default value for this parameter is the long host name of the local workstation. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

-webServerInstallPath *webserver_installpath_name*

The installation path of the Web server, local or remote. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

The default value for this parameter is dependent on the operating system of the local workstation and the value of the `webServerType` parameter. For example: AIX

```
webServerType=IHS: webServerInstallPath defaulted to "/usr/IBM/HTTPServer"
webServerType=IIS: webServerInstallPath defaulted to "n\a"
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to "/opt/sun/webserver"
webServerType=DOMINO: webServerInstallPath defaulted to "?"
webServerType=APACHE: webServerInstallPath defaulted to "?"
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to "n/a"
```

 HP-UX

```
webServerType=IHS: webServerInstallPath defaulted to "/opt/IBM/HTTPServer"
webServerType=IIS: webServerInstallPath defaulted to "n\a"
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to "/opt/sun/webserver"
```

```
webServerType=DOMINO: webServerInstallPath defaulted to ""
webServerType=APACHE: webServerInstallPath defaulted to ""
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to "n/a"
```

Linux

```
webServerType=IHS: webServerInstallPath defaulted to "/opt/IBM/HTTPServer"
webServerType=IIS: webServerInstallPath defaulted to "n\a"
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to "/opt/sun/webserver"
webServerType=DOMINO: webServerInstallPath defaulted to ""
webServerType=APACHE: webServerInstallPath defaulted to ""
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to "n/a"
```

Solaris

```
webServerType=IHS: webServerInstallPath defaulted to "/opt/IBM/HTTPServer"
webServerType=IIS: webServerInstallPath defaulted to "n\a"
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to "/opt/sun/webserver"
webServerType=DOMINO: webServerInstallPath defaulted to ""
webServerType=APACHE: webServerInstallPath defaulted to ""
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to "n/a"
```

Windows

```
webServerType=IHS: webServerInstallPath defaulted to "C:\Program Files\IBM\HTTPServer"
webServerType=IIS: webServerInstallPath defaulted to "C:\"
webServerType=SUNJAVASYSTEM: webServerInstallPath defaulted to "C:\"
webServerType=DOMINO: webServerInstallPath defaulted to ""
webServerType=APACHE: webServerInstallPath defaulted to ""
webServerType=HTTPSERVER_ZOS: webServerInstallPath defaulted to "n/a"
```

-webServerName *webserver_name*
> The name of the Web server. The default value for this parameter is
> webserver1. Use this parameter when creating profiles only. Do not supply this
> parameter when augmenting an existing profile.

-webServerOS *webserver_operating_system*
> The operating system from where the Web server resides. Valid values include:
> windows, linux, solaris, aix, hpux, os390, and os400. Use this parameter with
> the **webServerType** parameter.
>
> Use this parameter when creating profiles only. Do not supply this parameter
> when augmenting an existing profile.

-webServerPluginPath *webserver_pluginpath*
> The path to the plug-ins that the Web server uses. The default value for this
> parameter is *install_root*/plugins. Use this parameter when creating profiles
> only. Do not supply this parameter when augmenting an existing profile.

-webServerPort *webserver_port*
> Indicates the port from where the Web server will be accessed. The default
> value for this parameter is 80. Use this parameter when creating profiles only.
> Do not supply this parameter when augmenting an existing profile.

-webServerType *webserver_type*
> The type of the Web server. Valid values include: IHS, SUNJAVASYSTEM, IIS,
> DOMINO, APACHE, and HTTPSERVER_ZOS. Use this parameter with the
> **webServerOS** parameter. Use this parameter when creating profiles only. Do
> not supply this parameter when augmenting an existing profile.

Windows **-winserviceAccountType** `specifieduser | localsystem`
> The type of the owner account of the Windows service created for the profile.
> Use this parameter when creating profiles only. Do not supply this parameter
> when augmenting an existing profile.

Configuring **397**

Valid values include `specifieduser` or `localsystem`. The `localsystem` value runs the Windows service under the local account of the user who creates the profile. The default value for this parameter is `system`.

Windows **-winserviceCheck `true` | `false`**
The value can be either true or false. Specify `true` to create a Windows service for the server process that is created within the profile. Specify `false` to not create the Windows service. The default value for this parameter is `false`.

Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Windows **-winservicePassword** *winservice_password*
Specify the password for the specified user or the local account that is to own the Windows service. Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Windows **-winserviceStartupType `manual` | `automatic` | `disabled`**
Possible values for Windows service startup are:

* manual
* automatic
* disabled

The default value for this parameter is `manual`.

Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Windows **-winserviceUserName** *winservice_user_ID*
Specify your user ID so that the Windows operating system can verify you as an ID that is capable of creating a Windows service. Your user ID must belong to the Administrator group and have the following advanced user rights:

* Act as part of the operating system
* Log on as a service

The default value for this parameter is the current user name. The value for this parameter must not contain spaces or characters that are not valid such as the following: `*`, `?`, `"`, `<`, `>`, `,`, `/`, `\`, and `|`. The user that you specify must have the proper permissions to create a Windows service. You must specify the correct password for the user name that you choose.

Use this parameter when creating profiles only. Do not supply this parameter when augmenting an existing profile.

Configuring remote database support on IBM i

You can configure WebSphere Process Server to use a DB2 for i5/OS or DB2 for IBM i database residing remotely on an IBM i system. If you choose to use a remote database on IBM i for the product repository, then you must use DB2 for i5/OS or DB2 for IBM i as the database product.

About this task

You configure databases during the creation of a stand-alone server or deployment manager profile. When creating a custom profile, you must specify the same database product already configured for the deployment manager profile to which it will be federated.

You specify arguments on a series of Profile Management Tool pages that are used to run the manageprofiles command-line utility. Optionally, you can generate database definition scripts only and later have an administrator run them to create the DB2 collection and tables.

A number of components require database connectivity including:
- Failed Event Management
- Common Event Infrastructure
- Relationships
- Recovery
- Business Rules
- Business Space
- Selector
- Lock Manager
- Application Scheduler
- Service Integration (SI) Bus (Messaging Engines)
- Enterprise Service Bus (ESB) message logger

What to do next

Now, you can create a stand-alone profile or deployment manager profile to connect to a remote database.

IBM i database and collections

Unlike on distributed platforms, there is only one system-wide DB2 database on an IBM i system or logical partition. DB2 for i5/OS or DB2 for IBM i (depending on which version of the IBM i operating system you are using) is integrated with the IBM i operating system and is not a separate product that needs to be installed.

DB2 for i5/OS or DB2 for IBM i is the relational database that is fully integrated with the IBM i operating system, which makes it simple to use and manage.

The product also provides various functions and features, such as triggers, stored procedures, and dynamic bitmapped indexing, that serve a wide variety of application types. These applications range from traditional host-based applications to client/server solutions to business intelligence applications.

Here is the database hierarchy:
`(Single Database) > Schema name > Table name`

In a heterogeneous environment where WebSphere Process Server is running on a distributed platform, but accessing its Common database on an IBM i workstation, use the Toolbox for Java JDBC driver Type 4.

The driver file for the Toolbox JDBC driver is called `jt400.jar` and needs to be available on the workstation that is hosting WebSphere Process Server. You can obtain the driver for the distributed workstation in one of two ways:
- Copy the driver from the IBM i database workstation to a directory on the distributed workstation. The Toolbox JDBC driver file, `jt400.jar`, is found in a single, fixed location on IBM i: `/QIBM/ProdData/Http/Public/jt400/lib/jt400.jar`.

- Download the driver from the jtopen Web site to a directory on the distributed workstation. The jtopen Web site URL is at: http://sourceforge.net/projects/jt400.

Creating a stand-alone profile to connect to a remote database

The Profile Management Tool can create a configuration for one or more WebSphere Process Server stand-alone server profiles configured with a DB2 for i5/OS or DB2 for IBM i database on a remote IBM i server. The remote IBM i server hosting the DB2 for i5/OS or DB2 for IBM i database does not have WebSphere Process Server installed on it.

Before you begin

If your WebSphere Process Server installation resides on a Linux, UNIX, or Windows server and your database resides on a remote IBM i server, you must download the Toolbox for Java JDBC driver (jt400.jar) from the SourceForge.net Web site at https://sourceforge.net/projects/jt400 to a local temporary directory on the server hosting WebSphere Process Server.

Procedure

1. Follow the procedure to create an Advanced stand-alone server profile at "Creating **Advanced** stand-alone server profiles" on page 202. Do *not* create a Web server definition or a sample Business Process Choreographer.

   Note: Do not create the Web server definition using the Profile Management Tool. You must use the IBM HTTP Server for IBM i configuration and administration forms, which both create the Web server definition and an HTTP server instance. They also correctly associate the HTTP server to this Web server definition. For more information, see the topic Configuring an HTTP server instance in the WebSphere Application Server Network Deployment information center. Also, do not create a sample Business Process Choreographer. If you do so, a Derby rather than a DB2 for i5/OS or DB2 for IBM i database is created.

2. In the Database Configuration page, perform the following steps:

   a. Under **Choose a database product**, select the entry for the IBM i database product. This action sets the Common database and Common Event Infrastructure database names to *SYSBAS.

   b. Select **Delay execution of database scripts**. The profile creation process creates scripts that you or the database administrator must run manually on the remote IBM i server to create new databases and their required tables. It creates scripts for the Common and Common Event Infrastructure databases. The default locations for the databases are as follows:

      - **For the Common Event Infrastructure database:**

        – `Linux` `UNIX` *install_root*/profiles/*profile name*/dbscripts/CEI_*ceiDbName*

        – `Windows` *install_root*\profiles*profile name*\dbscripts\CEI_*ceiDbName*

      - **For the Common database:**

        – `Linux` `UNIX` *install_root*/profiles/*profile name*/dbscripts/CommonDB/*dbType*/*dbName*

        – `Windows` *install_root*\profiles*profile name*\dbscripts\CommonDB*dbType**dbName*

To store the database creation and configuration scripts in a location other than the default location, select the **Override the destination directory for generated scripts** check box and designate your new location in the **Database script output directory** field.

    c. Select **Use this database for Messaging Engines (MEs)**.

    d. Click **Next**.

3. In the Database Configuration (Part 2) panel, perform the following steps:

    a. Enter a valid User Name and Password to authenticate to the remote database.

    b. Enter the Location (directory) of the JDBC driver class path files (jt400.jar).

    c. Enter the Database server host name (for example IP address) of the IBM i server where the remote DB2 for i5/OS or DB2 for IBM i database is located.

    d. Enter the Database collection name, WPRCSDB by default. The first three characters of this name must be unique for the database that is being hosted on the remote IBM i server.

    e. Click **Next**.

4. When profile creation completes, on the Profile Summary page, clear the **Launch the First steps console** option and click **Finish**. Also, close the Profiles page, which is open in a separate window.

5. Export the DDL for both the Common Event Infrastructure and the Common databases to the remote IBM i system. The DDL, in the form of generated database scripts, are in locations you specified earlier on the Database Configuration page. You can provide the scripts by a number of different methods to the database administrator.

6. The administrator must run the Common Event Infrastructure and Common database scripts to set up the remote DB2 database tables for the databases.

Results

You have created a stand-alone profile to connect to a remote database.

DB2 for i5/OS or DB2 for IBM i tables and collections have been generated on a remote IBM i system for CEI, Business Process Choreographer, Common database, Service Integration Bus, and WebSphere Enterprise Service Bus Message Logger.

What to do next

Start the server. See instructions at Starting stand-alone servers.

Creating a deployment manager profile to connect to a remote database

The Profile Management Tool can create a WebSphere Process Server deployment manager profile configured with a DB2 for i5/OS or DB2 for IBM i database on a remote IBM i server. The remote IBM i server hosting the DB2 for i5/OS or DB2 for IBM i database does not have WebSphere Process Server installed on it.

Before you begin

If your WebSphere Process Server installation resides on a Linux, UNIX, or Windows server and your database resides on a remote IBM i server, you must download the Toolbox for Java JDBC driver (jt400.jar) from the SourceForge.net

Web site at https://sourceforge.net/projects/jt400 to a local temporary directory on the server hosting WebSphere Process Server.

Procedure

1. Follow the procedure to create an Advanced deployment manager profile at "Creating **Advanced** deployment manager profiles" on page 214.

2. In the Database Configuration page, perform the following steps:

   a. Under **Choose a database product**, select the entry for the IBM i database product. This action sets the Common database name to *SYSBAS.

   b. Select **Delay execution of database scripts**. The profile creation process creates scripts that you or the database administrator must run manually on the remote IBM i server to create the Common database and its required tables. The default location for the database is as follows:

      - � Linux ▪ UNIX *install_root*/profiles/*profile name*/dbscripts/CommonDB/*dbType*/*dbName*

      - ▪ Windows *install_root*\profiles*profile name*\dbscripts\CommonDB\ *dbType**dbName*

      To store the database creation and configuration scripts in a location other than the default location, select the **Override the destination directory for generated scripts** check box and designate your new location in the **Database script output directory** field.

   c. Click **Next**.

3. In the Database Configuration (Part 2) panel, perform the following steps:

   a. Enter a valid User Name and Password to authenticate to the remote database.

   b. Enter the Location (directory) of the JDBC driver class path files (jt400.jar).

   c. Enter the Database server host name (for example IP address) of the IBM i server where the remote DB2 for i5/OS or DB2 for IBM i database is located.

   d. Enter the Database collection name, WPRCSDB by default. The first three characters of this name must be unique for the database that is being hosted on the remote IBM i server.

   e. Click **Next**.

4. When profile creation completes, on the Profile Summary page, clear the **Launch the First steps console** option and click **Finish**. Also, close the Profiles page, which is open in a separate window.

5. Export the DDL for the Common database to the remote IBM i system. The DDL, in the form of generated database scripts, are in location you specified earlier on the Database Configuration page. You can provide the scripts by a number of different methods to the database administrator.

6. The administrator must run the Common database scripts to set up the Common database.

Results

You have created a deployment manager profile to connect to a remote database. DB2 for i5/OS or DB2 for IBM i tables and collections have been generated on a remote IBM i system for Business Process Choreographer, Common database, Service Integration Bus, and WebSphere Enterprise Service Bus Message Logger.

What to do next

Start the deployment manager.

Use the administrative console to configure Business Process Choreographer.

In a deployment environment, you must create and configure other databases, create custom profiles and federate them to your deployment manager, create servers, create clusters if you want workload management capabilities, and perform other tasks specific to your planned installation environment. Your planned environment dictates which tasks you must perform and the order in which you perform them.

Deleting profiles using the manageprofiles command-line utility

You can delete a profile from the command line using the manageprofiles command-line utility.

Before you begin

For more information about the manageprofiles command-line utility, see "manageprofiles command-line utility" on page 375.

Procedure

1. Open a command prompt and run one of the following commands, based on your operating system:

   - `Linux` `UNIX` `manageprofiles.sh -delete -profileName` *profile_name*
   - `Windows` `manageprofiles.bat -delete -profileName` *profile_name*

   The variable *profile_name* represents the name of the profile that you want to delete.

2. Confirm that the profile deletion has completed by checking the following log file:

   - `Linux` `UNIX` *install_root*/logs/manageprofiles/ *profile_name*_delete.log
   - `Windows` *install_root*\logs\manageprofiles*profile_name*_delete.log

Configuring databases

Includes information about database configuration for the Common database, Common Event Infrastructure, Business Process Choreographer, enterprise service bus logger mediation, messaging engine, selector and business rules group, and DB2 message logger database on a remote z/OS system.

To plan your database configuration, you must know the components that you will use. Table 165 on page 404 lists the WebSphere Process Server components that require a database table and the default names of the databases where the tables associated with these components are stored.

Note: You can change these names if you choose.

Table 165. Databases required by individual components

Server component	Database (default name)	Notes®
Business Process Choreographer	BPEDB	The BPEDB needs to be created before you start a server or cluster with Business Process Choreographer configured.
Business Process Choreographer Explorer reporting function	OBSRVDB	You can use the Business Process Choreographer Explorer reporting function to create reports on processes that have been completed.You can use a separate database for Business Process Choreographer Explorer reporting and default the name to OBSRVDB. **Note:** The BPEDB needs to be created before you start a server or cluster with Business Process Choreographer configured. For production environments, it is encouraged to have dedicated databases. For instance, use BPEDB as the database for the Business Process Choreographer and use the OBSRVDB as the database for Business Process Choreographer explorer reporting data.
Business Space	WPRCSDB (the Common database)	For stand-alone profiles, you must create the Common database before you start WebSphere Process Server. For other profiles, you must use the administrative console to configure Business Space. Configuring a Business Space database is mandatory for using Business Space powered by WebSphere, which provides a common interface for application users to create, manage and integrate Web interfaces across the IBM WebSphere Business Process Management portfolio.
Common Event Infrastructure	EVENT (stores events)	You do not need to create this database before you start WebSphere Process Server, but it is mandatory for the monitoring of events.

Table 165. Databases required by individual components (continued)

Server component	Database (default name)	Notes®
Relationships	WPRCSDB (the Common database)	You must create the Common database before you start WebSphere Process Server. **Note:** The WPRCSDB tables need to be configured either during the start up of the deployment manager or stand-alone server or before starting the deployment manager or stand-alone server.
Mediation	WPRCSDB (the Common database)	You must create the Common database before you start WebSphere Process Server. **Note:** The WPRCSDB tables need to be configured either during the start-up of the deployment manager or stand-alone server or before starting the deployment manager or stand-alone server.
Recovery	WPRCSDB (the Common database)	You must create the Common database before you start WebSphere Process Server. **Note:** The WPRCSDB tables need to be configured either during the start-up of the deployment manager or stand-alone server or before starting the deployment manager or stand-alone server.
Application scheduler	WPRCSDB (the Common database)	You must create the Common database before you start WebSphere Process Server. **Note:** The WPRCSDB tables need to be configured either during the start-up of the deployment manager or stand-alone server or before starting the deployment manager or stand-alone server.

Table 165. Databases required by individual components (continued)

Server component	Database (default name)	Notes®
Selectors/Business rules	WPRCSDB (the Common database)/Repository DB	You must create the Common database before you start WebSphere Process Server. **Note:** The WPRCSDB tables need to be configured either during the start-up of the deployment manager or stand-alone server or before starting the deployment manager or stand-alone server.
SIBus	User created	These tables need to be configured either during the startup of the messaging engine or before starting the messaging engine. You can use a file store with SIBus in a stand-alone environment during profile creation. However, you can not use a file store with SIBus in a network deployment environment.
Enterprise service bus	EsbLogMedDB	These tables need to be configured either during startup of the deployment manager or stand-alone server or before starting deployment manager or stand-alone server .

Identifying required database administrator tasks

All of the database creation and configuration tasks that require database administrator (DBA) action are listed below.

Choosing a database

Choosing a database

Database privileges and security considerations

- "Database privileges" on page 407
- Identifying necessary security authorizations

Creating a network deployment configuration

"Creating a Network Deployment configuration" on page 156

Profile creation

- "Prerequisites for creating or augmenting profiles" on page 189
- "Creating profiles using the Profile Management Tool" on page 197
- "Creating Deployment environment deployment manager profiles" on page 220

Note: Database administrator privileges are required for the database configuration panels that are part of creating a deployment manager profile for a deployment environment. If you plan to use the deployment environment feature, and want to use a database other than Derby Network Server as your database product, the user ID you provide for the **User name to authenticate with the database** field on the database configuration panels must have DBA privileges.

Database configuration

- "Configuring the Common database and the Common Event Infrastructure database using the Profile Management Tool" on page 240
- Create the database and tables before profile creation or augmentation
  - "Creating the Common database manually before product installation" on page 31
  - "Creating the database design file using the database design tool" on page 431

  "Creating the Common database manually before product installation" on page 31
- Create the database and tables after profile creation or augmentation
  - "Creating tables on an existing Common database after profile creation or augmentation" on page 417
  - "Creating the Common database and tables after profile creation or augmentation" on page 416
  - "Creating the database design file using the database design tool" on page 431
- "Messaging engine database configurations" on page 421

Relevant links

- "Configuring Common Event Infrastructure" on page 591
- Configuring Business Process Choreographer
- "Configuring Business Space" on page 484
- Configuring WebSphere Business Monitor
  - Database considerations
  - Installing the database
- "Table and schema creation matrices" on page 443
- "Creating Common Event Infrastructure and Common database repositories in DB2 on a remote z/OS server" on page 420

Database privileges

Use database privileges to determine the authority required to create or access your data store tables for each supported database management system.

When you create your schemas using Installer, Profile Management Tool or scripts, you must have a user ID with enough authority to create your tables. Once the tables are created, the applications must have enough authority to select, insert, update, and delete information in the tables.

Table 166 on page 408 describes the database privileges needed to access the data store.

Table 166. Database privileges

Database management system	Minimum privilege required to use the data store tables	Additional privilege required to create the data store tables
DB2	The user ID must SELECT, INSERT, UPDATE, and DELETE privileges on the tables.	The user ID requiresCREATETAB authority on the database and USE privilege on the table space as well as CREATEIN privilege on the schema.
Oracle	The user ID requires the SESSION privilege to connect to the database. If the same user ID owns both the data store schema, and the component that is connecting to the database, the user ID has sufficient privilege to manipulate the tables. Otherwise, the user ID requires SELECT, INSERT, UPDATE and DELETE object privileges on the tables that make up the data store, and DROP ANY TABLE system privilege to enable use of the TRUNCATE TABLE statement. You must create the Oracle database using a UTF-8 character set, which supports the other customer character sets that are supported by WebSphere Process Server.	The user ID requires sufficient privilege to create relational tables and indexes in the data store schema. The database also requires a space quota in the default table space of the owner of that schema. Refer to Table 167 on page 409 for additional Oracle database privileges for WebSphere Process Server and WebSphere Enterprise Service Bus components.
SQL Server	Configure the SQL Server for SQL Server and Windows authentication. This allows authentication to be based on an SQL server login ID and password. The user ID can be the owner of the tables, or be a member of a group that has sufficient authority to issue TRUNCATE TABLE statements.	The user ID requires CREATE TABLE statement privilege.
Informix	The user ID must have CONNECT privilege on the database. It must also have SELECT, INSERT, UPDATE, and DELETE authority on the tables.	The user ID must have RESOURCE privilege on the database.
Derby	If user authentication is enabled, you must authorize the user ID to access the database.	You require no additional privileges.

Table 167 describes additional Oracle database privileges for WebSphere Process Server and WebSphere Enterprise Service Bus components.

Note: If you are configuring all the following components for a single Oracle database, you can create a superset of all the privileges that are specified for each component. If the four components are being configured for numerous databases, you can set different privileges for each.

Table 167. Additional Oracle database privileges

Component	Configuration privileges	Runtime privileges
Common DB	CREATE TABLE, CREATE INDEXTYPE, ALTER TABLE, INSERT, CREATE SEQUENCE, CREATE USER, ALTER USER, CREATE TABLESPACE	SELECT, UPDATE, DELETE, INSERT, CREATE VIEW, CREATE PROCEDURE
Business Process Choreographer	CREATE TABLE, ALTER TABLE, CREATE VIEW, CREATE TABLESPACE, CREATE USER, CREATE PROCEDURE	SELECT, UPDATE, DELETE, INSERT
Common Event Infrastructure (CEI)	CREATE TABLE, CREATE INDEXTYPE, ALTER TABLE, CREATE VIEW, ALTER SESSION, SELECT, UPDATE, DELETE, INSERT, CREATE TABLESPACE, CREATE PROFILE CREATE ROLE, CREATE PROCEDURE, CREATE TEMPORARY TABLESPACE	SELECT, UPDATE, DELETE, INSERT, CREATE PROCEDURE
Messaging Engines	CREATE TABLE, CREATE INDEXTYPE	SELECT, UPDATE, DELETE, INSERT, DROP ANY TABLE

For additional assistance when configuring WebSphere Process Server to work with an Oracle database, refer to the following tutorial: http://publib.boulder.ibm.com/infocenter/dmndhelp/v7r0mx/topic/com.ibm.websphere.wps.doc/doc/tins_oracleincorp.html.

Component-specific database configurations

The topics in this section provide WebSphere Process Server component-specific database configuration information.

CommonDB database configurations

The Common database configurations contain information about supported database types; scripts and their locations; profile creation configuration actions; installation parameters; types of created tables and user ID privileges.

The Common database is optionally created when you create a WebSphere Process Server profile. This database acts as a repository for various components.

The WebSphere Process Server Common database is used by the following product components:
• Recovery
• Relationship service

- Mediation
- Application Scheduler
- Customization (selector and business rule group)
- EventSequencing (LockManager)
- Enterprise Service Bus (ESB) Logger Mediation Primitive

You can create the Common database before, during, or after WebSphere Process Server profile creation.

- Choose one of the following methods to create the database tables before configuring WebSphere Process Server:
  - Edit and run the default scripts that come with WebSphere Process Server. Refer to "Creating the Common database manually before product installation" on page 31.

    Note: The default scripts can only be used to create the CommonDB and Business Process Choreographer tables.
  - Use the design file that was created using the database design tool (DDT). Refer to "Creating the database design file using the database design tool" on page 431.
- Choose one of the following methods to create the database tables after configuring WebSphere Process Server:
  - Use the Profile Management Tool to configure WebSphere Process Server to work with the tables in the database as you create the profile. You will be able to create and configure the database tables during profile creation, or delay creation and configuration until after. The Profile Management Tool generates database scripts that you can use after to create and configure the database tables. These generated scripts are ready to use. No editing is required.
  - Use the design file that was created using the database design tool (DDT). Refer to "Creating the database design file using the database design tool" on page 431.

Supported database types

The Common database can use the following database products:

Table 168. Supported database products

Database Types	Considerations
Derby Embedded or Derby Embedded 40	Used as the default database type for standalone profile.
Derby Network Server or Derby Network Server 40	Used as the default database type in network deployment environment.
DB2 Universal	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 Data Server	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.

Table 168. Supported database products (continued)

Database Types	Considerations
DB2 for z/OS v8 DB2 for z/OS v9	**Important:** When creating a profile for a server that uses DB2 for z/OS v9, the server must be able to connect to the DB2 database.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 UDB for iSeries (Toolbox) DB2 for i5/OS (Toolbox)	Used as a remote database for network deployment environment or as a local database for a standalone profile.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
Informix Dynamic Server	
Microsoft SQL Server (DataDirect)	
Microsoft SQL Server (Microsoft)	
Oracle	You need sysdba privilege to create the database, tables and schemas. Failure to have the correct sysdba privilege can result in errors creating and accessing the tables and schemas.

User ID privileges

The user credentials that you provide in the Profile Management Tool must have the permissions necessary to create table spaces, tables, schemas, indexes, and stored procedures. For the Create new database option, the user identity must have the necessary privileges to create a new database. See "Users and schemas for databases" and "Database privileges" for more information.

Note: If the user running the script has enough authority to create tables, the script will not require an authentication ID within the script.

Database Management Service instances

There is one set of common database tables per cell.

Configuration actions during profile creation

There are four options for installing the Common database:
- Installer
- Profile Management Tool
- Silent installation
- Scripts

Within each of these options are several more choices.

Installer

Use the Installer if you are going to create your profiles when you install your software. You can install your database products during installation but you are limited in the types of database products you can install. If you want to use another supported database product not in Table 169, you must create your deployment manager using the Profile Management Tool.

Table 169. Installer options

Option	Databases you can use
Typical: Stand-alone profile	Derby Embedded or Derby Embedded 40 only
Typical: all other profiles	Derby Network Server or Derby Network Server 40 only
Customized: Stand-alone profile	• Derby Network Server or Derby Network Server 40 • DB2 Universal • DB2 Data Server • Oracle
Customized: all other profiles	• Derby Network Server or Derby Network Server 40 • DB2 Universal • DB2 Data Server • Oracle

A typical installation uses default values for configuration parameters and you cannot change these defaults. If you choose a customized installation, the defaults can be changed for your specific requirements. See "InstallingWebSphere Process Server and creating a profile interactively" for more information.

Profile Management Tool

Use the Profile Management Tool to create profiles after you install your software. The Profile Management Tool allows you the options of installing your database before, during or after profile creation. See "Creating the Common database and tables manually after profile creation or augmentation" for more information. For the locations of the database scripts, see "Scripts and their locations".

Table 170 lists the databases supported by typical (default) profiles and customized profiles. The Profile Management Tool typical installation has default values for the database and configuration parameters that cannot be changed. The Profile Management Tool customized installation allows you to change the configuration parameters and to choose a supported database. See "Creating profiles" for more information on creating customized profiles.

Table 170. Profile Management Tool options

Options	Databases you can use
Typical: Stand-alone profile	Derby Embedded or Derby Embedded 40 only
Typical: all other profiles	Derby Network Server or Derby Network Server 40 only
Customized: Stand-alone profile	Any of the "Supported database types" on page 410
Customized: all other profiles	Any of the "Supported database types" on page 410

Profile Management Tool allows you to augment an existing profile from previous versions of

- WebSphere Process Server
- WebSphere Application Server
- WebSphere ESB

See "Augmenting existing profiles" for more information.

Silent Installations

When you install the product silently, you can specify the common database configuration by editing the template response file. See "Installing silently" for more information.

Scripts

There are two location where you can find the default profile scripts. You can locate one set of default scripts on your product media in the following directory `media_root/dbscripts`.

The other profile default scripts are located in the following directory after installation of WebSphere Process Server `install_root/dbscripts/CommonDB/dbType`.

You can create your common database using scripts before you install WebSphere Process Server or during profile creation. See "Creating the Common database manually before product installation" for more information.

If you choose to configure your database with scripts during profile creation, you first need to install WebSphere Process Server and select the option to defer database creation. Profile creation collects your database parameters, which are added to default scripts. After you complete your profile creation, you can find the updated scripts in the following location:

`profile_root/dbscripts/CommonDB/dbType/dbName`

You can then give these scripts to the person who will create your Common database. The scripts are ready to execute, but you can edit them to include any specific requirements. If you try to start WebSphere Process Server before creating the database you will receive an error message.

The scripts perform the following steps:

- Create a new database, if asked (valid only for a local database), depending on your choices in the Database configuration panel in the Profile Management Tool. See "Restrictions" on page 415 for details on database commands that are not supported by the Profile Management Tool.

  Note: Even though you can defer creation of the database until after the profile creation is complete, it is necessary to enter valid information in the Database configuration panel of the Profile Management Tool. This information is used to create the data source for the WebSphere Process Server.
- Create the data source on the JDBC provider.

Note: If you are creating the database at the same time as the profile any mistakes in the database parameters that you provide will yield errors in the overall profile creation. However, if you are delaying the database creation, the profile will be created without errors, but the generated database scripts will contain errors and therefore must be edited before the database can be created.

Note: For nodes of a cell, you must select the same database type as the deployment manager profile. The data source is maintained only at the cell level.

SQL scripts

SQL scripts allow you to configure your database before or after profile creation. Tables are created with a deployment manager profile and so there are no SQL scripts executed as part of managed node creation.

SQL scripts for each Common database client can be found in the following locations:
- *media_root/dbscripts* on your product media
- *install_root*/dbscripts/CommonDB/*dbType* after you install WebSphere Process Server

If you choose to defer creation of the database after you have created the profile, the updated scripts will be found in:

profile_root/dbscripts/*feature*/*dbType*/*dbName*

The SQL script naming convention is:
- For a component-specific script: `createTable_`*componentName*`.sql`. For example `createTable_Recovery.sql`.
- For a component independent script: `createTable.sql`.

The script naming convention is shown in Table 171.

Table 171. Common database script naming convention

Type of script	Script name
Component specific	*scriptName_componentName*.sql
Component independent	*scriptName*.sql

JDBC provider

A new JDBC provider is created depending on the database type. The provider is created in the node scope in a stand-alone profile and at cell level in network deployment environment. JDBC Provider refers to variable `JDBC_DRIVER_PATH` to locate local JDBC drivers. The variable is specified in cell level and each node level to point to correct local path.

Data source name:
- `WPS DataSource`

Data source JNDI name:
- `jdbc/WPSDB`

Restrictions

There are several restrictions on the database commands that are available to the user during profile creation.

Create new database is disabled for the following database types:

- DB2 for z/OS v8
- DB2 for z/OS v9
- Oracle

Tables

The Common database scripts create only static tables during profile creation. The following table gives a list of all the tables that are created by different components.

Table 172. Tables created by WebSphere Process Server components

Component	Table names	Scripts
Recovery	FAILEDEVENTS FAILEDEVENTBOTYPES FAILEDEVENTMESSAGE	`createTable_Recovery.sql`
Mediation	MEDIATION_TICKETS	`createTable_mediation.sql`
Relationship	Dynamic table, created at runtime	`createTable_Relationship MetadataTable.sql`
Application Scheduler	WSCH_LMGR WSCH_ LMPR WSCH_TASK WSCH_TREG	`createTable_AppScheduler.sql`
Customization (selector/business rule group)	BYTESTORE BYTESTOREOVERFLOW APPTIMESTAMP	`createTable_customization.sql`
Common database	SchemaVersionInfo	`createTable_CommonDB.sql`
Persistent LockManager	PERSISTENTLOCK	`createTable_lockmanager.sql`
ESB Logger Mediation	MSGLOG	`createTable_ESBLogger Mediation.sql`

All the above SQL scripts are executed by commonDBUtility.ant from each component script, such as **configRecovery** > **commonDBUtility** > **execute createTable_Recovery.sql**. When the value **delayConfig=true** is in the response file, the SQL files are created, but are not run. When this is the case, you will need to run the SQL manually after the configuration.

Note: In the ESB Logger Mediation component, you can configure each message logger primitive to use a different data source and a different database.

Exported scripts

Scripts are created for any option chosen on the Profile Management Tool panel to configure the Common database. The scripts contain only basic creation statements for databases, tables, and indexes. The database administrator must use database native commands to execute these scripts. See "Configuring the Common database using the Profile Management Tool" for more information.

The scripts are called configCommonDB.bat or configCommonDB.sh for Windows and UNIX-based operating systems, respectively.

Database scripts are exported to the following folder:

profile_root/dbscripts/CommonDB/*dbType*/*dbName*

Creating the Common database and tables after profile creation or augmentation:

If you postponed creating the Common database and its tables by selecting the **Delay execution of database scripts (must select if using a remote database)** check box on the Database configuration panel in the Profile Management Tool, you or your database administrator must create the database and its tables manually. You can do this using scripts that the Profile Management Tool generates during profile creation or augmentation.

Before you begin

This topic assumes that you created or augmented a stand-alone server or deployment manager profile using the Profile Management Tool. It also assumes that in the Database configuration panel in the Profile Management Tool, you selected the **Create a new local database** radio button and chose to delay creation of the Common database and its tables by selecting the **Delay execution of database scripts (must select if using a remote database)** check box.

About this task

Because a WebSphere Process Server installation requires the Common database to function, if you did not allow the Profile Management Tool to create it automatically, you or your database administrator must now create the database and its tables manually by using scripts that the Profile Management Tool generated during the profile creation or augmentation.

Procedure
1. Go to the directory containing the configCommonDB script on i5/OS platforms, the configCommonDB.sh script on Linux and UNIX platforms, or the configCommonDB.bat script on Windows platforms. You specified its location in the **Database script output directory** field on the Database configuration panel in the Profile Management Tool. By default, this location is:
   - **On i5/OS platforms:** *profile_root*/dbscripts/CommonDB/*db_type*/*db_name*
   - Linux   UNIX   *profile_root*/dbscripts/CommonDB/*db_type*/*db_name*
   - Windows   *profile_root*\dbscripts\CommonDB*db_type**db_name*

   The variable *db_type* represents the supported database product and *db_name* represents the name of the database.

   You must pass the **createDB** parameter to the configCommonDB script if you want to create a new local database; otherwise an existing database will be used. For example:

   configCommonDB.sh createDB - create tables in a new database

   configCommonDB.sh - create tables using an existing database

   Important: You need to have *SECOFR authority on the IBM i system before you can run these scripts.

2. Use your standard database definition tools, native commands, and procedures to create the database and required tables by running this script. The script contains only basic statements for creating databases, tables, and indexes.

What to do next

After database creation completes successfully, before starting the server or deployment manager, be sure the database is running even if it is installed locally. Then start the server or deployment manager from the profile's First steps console to ensure there are no errors. You can check the `SystemOut.log` and `SystemErr.log` files for errors. These files are found in the following locations:

- *profile_root*/logs/*server_name*, for a stand-alone profile
- *profile_root*/logs/dmgr, for a deployment manager profile

Creating tables on an existing Common database after profile creation or augmentation:

If you postponed creating required tables for your existing Common database by selecting the **Delay execution of database scripts (must select if using a remote database)** check box on the Database configuration panel in the Profile Management Tool, you or your database administrator must create the tables manually. You can do this using scripts that the Profile Management Tool generates during profile creation or augmentation.

Before you begin

This topic assumes that you created or augmented a stand-alone server or deployment manager profile using the Profile Management Tool. It also assumes that in the Database configuration panel in the Profile Management Tool, you selected the **Use an existing database** radio button and chose to delay creation of the tables by selecting the **Delay execution of database scripts (must select if using a remote database)** check box.

About this task

Because a WebSphere Process Server installation requires the Common database and its tables to function, if you did not allow the Profile Management Tool to create the tables automatically, you or your database administrator must now create the tables manually by using scripts that the Profile Management Tool generated during the profile creation or augmentation.

Procedure

1. Go to the directory containing the table creation script createDBTables on i5/OS platforms, createDBTables.sh on Linux and UNIX platforms, or createDBTables.bat on Windows platforms. You specified its location in the **Database script output directory** field on the Database configuration panel in the Profile Management Tool. By default, this location is:

   - **On i5/OS platforms:** *profile_root*/dbscripts/CommonDB/*db_type*/*db_name*

   - `Linux` `UNIX` *profile_root*/dbscripts/CommonDB/*db_type*/*db_name*

   - `Windows` *profile_root*\dbscripts\CommonDB*db_type**db_name*

   The variable *db_type* represents the supported database product, and *db_name* represents the name of the database.

2. Use your standard database definition tools, native commands, and procedures to create the required tables by running this script. The script contains only basic statements for creating databases, tables, and indexes.

What to do next

After the tables are created successfully, before starting the server or deployment manager, be sure the database is running even if it is installed locally. Then start the server or deployment manager from the profile's First steps console to ensure there are no errors. You can check the `SystemOut.log` and `SystemErr.log` files for errors. These files are found in the following locations:

- *profile_root*/logs/*server_name*, for a stand-alone profile
- *profile_root*/logs/dmgr, for a deployment manager profile

Common Event Infrastructure database configurations

The Common Event Infrastructure database specifications list the types of supported databases, script locations, profile configuration types, and necessary User ID privileges.

Use the Common Event Infrastructure database to store events that are captured when monitoring WebSphere Process Server.

You create the Common Event Infrastructure database for a stand-alone profile by default and for each instance of a Common Event Infrastructure server in a network deployment environment. To create the database, you can use the installation procedure, the Profile Management Tool or the administrative console.

Note: You must configure WebSphere Process Server to use the tables. This is done using either the Profile Management Tool (stand-alone profile only), or through the administrative console (deployment environments). Refer to "Configuring Common Event Infrastructure" on page 591.

The Common Event Infrastructure database is an internal device and you do not interact directly with it. All interactions with the Common Event Infrastructure database must be performed using the supported Common Event Infrastructure APIs.

For more information about configuring the Common Event Infrastructure database, see the topic *Configuring the event database* in either of the following locations:

- *WebSphere Process Server for Multiplatforms, version 6.1.2 Common Event Infrastructure* PDF
- The WebSphere Process Server for Multiplatforms online information center at Configuring the event database

User ID privileges

The user credentials that you provide in the Profile Management Tool must have the permissions necessary to create table spaces, tables, schemas, indexes, and stored procedures. For the Create new database option, the user identity must have the necessary privileges to create a new database. See "Users and schemas for databases" and "Database privileges" for more information.

Note: If the user running the script has enough authority to create tables, the script will not require an authentication ID within the script.

Database Management Service instances

Each deployment target of the Common Event Infrastructure server has one database. The Common Event Infrastructure database is only created for a stand-alone server profile so there is one instance of the Database Management Service (DBMS) for each server.

Configuration actions during profile creation

How the Common Event Infrastructure is created depends on the type of environment:

Standalone Environment

Configuration of the Common Event Infrastructure database is done as part of the profile creation by the profile template Apache Ant script `configCei.ant`. This script invokes the Common Event Infrastructure administrative tasks with all the necessary properties for the desired configuration.

In the stand-alone environment, the event database and tables are created, and scripts are exported to `profile_root/dbscripts/CEI_event` by default. If you use the optional **outputScriptDir** parameter, the default location of the scripts is `profile/databases/event/`*node*`/`*server*`/dbscripts/`*dbtype*.

In the Profile Management Tool or when you use manageprofiles command-line utility, the default location for standalone CEI environment `profile_root/dbscripts/`*CEI_DBNAME*.

Network Deployment Environment

In the Network Deployment Environment, the deployment manager profile creation or managed profile creation does not include the automatic creation of the Common Event Infrastructure database. To create the Common Event Infrastructure database, see "Configuring the event database."

For Network Deployment, you must configure the Common Event Infrastructure server through the Administrative console. For more information, see "Configuring the Common Event Infrastructure"

Common Event Infrastructure provides an administrative task configEventServiceDB to:
- Create event database and tables by setting the createDB parameter to true
- Export the SQL scripts by setting the createDB parameter to false

SQL scripts

Common Event Infrastructure provides an administrative task **configEventService**<*DBTYPE*>**DB** to:
- Create event database and tables by setting the createDB parameter to true
- Export the SQL scripts by setting the createDB parameter to false

In standalone environment, the event database and tables are created, and scripts are exported to `profile_root/dbscripts/CEI_event` directory.

JDBC provider

The Common Event Infrastructure administrative task
configEventService*DBTYPE*DB creates the JDBC provider and the data sources.
The format is `profile_root/databases/event/`*deployment_environment*`/dbscripts/`
dbName directory where *deployment_environment* is either a cluster or server.

The JNDI names of the components are:

`jndiName="jdbc/cei"`

`jndiName="jdbc/eventcatalog"`

Data source names are:
- event
- eventcatalog

The scripts that are used for creating the JDBC provider for the Common Event
Infrastructure database are stored in the following location: *configuration_root/*
app_server_root/profiles/profilename/event/dsscripts/${dbtype}

Tables

Many tables are created. Look under the generated scripts to see which tables are
generated for the given database product.

Exported scripts

Shell scripts are created in the following directory to be used to run the generated
SQL scripts.

configuration_root/app_server_root/profiles/profilename/event/dbscripts/dbtype

**Creating Common Event Infrastructure and Common database repositories in
DB2 on a remote z/OS server:**

If you plan to use DB2 on a remote z/OS workstation for the Common Event
Infrastructure and Common database repositories, you or the database
administrator (DBA) must create relevant databases and correct storage groups on
the z/OS workstation.
- To create the Common Event Infrastructure repository, see Configuring the event
  database and its subtopics.
- To create the Common database repository, use standard database definition
  tools and procedures to edit and run the default scripts provided in the
  following directories:
  - `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root/*
    `dbscripts/CommonDB/DB2zOSV8/`
  - `Windows` **On Windows platforms:** *install_root*`\dbscripts\CommonDB\`
    `DB2zOSV8\`
  - `Linux` `UNIX` **On Linux and UNIX platforms:** *install_root/*
    `dbscripts/CommonDB/DB2zOSV9/`
  - `Windows` **On Windows platforms:** *install_root*`\dbscripts\CommonDB\`
    `DB2zOSV9\`

These same scripts are also provided in the *media_root* or *extraction_root/* `dbscripts` directory. For more information on how to edit the scripts, see "Creating the DB2 database for z/OS" on page 35.

Business Process Choreographer database configurations

You must configure Business Process Choreographer on a server or cluster before you install any enterprise applications that contain business processes, human tasks, or both.

For detailed information on how to Configure the Business Process Choreographer database, refer to Configuring Business Process Choreographer.

Messaging engine database configurations

The messaging engine database specifications lists supported database type; scripts and their locations; profile creation types; and necessary user ID privileges.

The messaging engine database is used to store operating information. Also stored are essential objects that the messaging engine needs for recovery in the event of a failure.

The messaging engine database is used by the message engines for Service Component Architecture (SCA), Business Process Choreographer, and Common Event Infrastructure. The default database name for the SCA messaging engine is SCADB, for the other messaging engines it is MEDB. For the Derby Embedded or Derby Embedded 40 database, each messaging engine will have its own database or schema. The default schema name is IBMWSSIB.

Note: Multiple schemas are not supported by all database types, refer to your database documentation for details.

In a standalone environment, you can configure your SCA messaging engine using the administrative console **Servers -> Application servers ->** *server* **-> Business integration -> Service component architecture** configuration page. In a patterned network environment, the messaging engines are configured during installation. However, for a custom network environment, you need to configure the messaging engines manually. See "Custom deployment environment layout configuration" for more information.

You have a lot of control over the messaging engine databases, for example, you can create a database for each messaging engine or you can use a single database for all the messaging engines. Each messaging engine must have either its own database or schema.

Supported Database Types

The messaging engine database can use the following database products:

Table 173. Supported database products

Database Types	Considerations
Derby Embedded or Derby Embedded 40	Used as the default database type for standalone profile.
Derby Network Server or Derby Network Server 40	Used as the default database type in network deployment environment.

Table 173. Supported database products (continued)

Database Types	Considerations
DB2 Universal	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 Data Server	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 for z/OS v8 DB2 for z/OS v9	**Important:** When creating a profile for a server that uses DB2 for z/OS v9, the server must be able to connect to the DB2 database.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 UDB for iSeries (Toolbox) DB2 for i5/OS (Toolbox)	Used as a remote database for network deployment environment or as a local database for a standalone profile.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
Informix Dynamic Server	
Microsoft SQL Server (DataDirect)	
Microsoft SQL Server (Microsoft)	
Oracle	You need sysdba privilege to create the database, tables and schemas. Failure to have the correct sysdba privilege can result in errors creating and accessing the tables and schemas.

User ID privileges

The user credentials that you provide in the Profile Management Tool must have the permissions necessary to create table spaces, tables, schemas, indexes, and stored procedures. For the Create new database option, the user identity must have the necessary privileges to create a new database. See "Users and schemas for databases" and "Database privileges" for more information.

Note: If the user running the script has enough authority to create tables, the script will not require an authentication ID within the script.

For network deployment environment, you need all necessary permissions for user privileges specified during configuration from the administrative console.

Note: For DB2 Version 9.7, you must manually grant the newly created user the appropriate authority because the user creation does not automatically grant the user the necessary authority.

Database Management Service (DBMS) instances

Each messaging engine has its own database or schema:

- One is used to host each messaging engine for the Service Component Architecture system bus.
- Another is used to host each messaging engine for the Service Component Architecture application bus.
- Another is used to host each messaging engine for the Common Event Infrastructure bus.
- Another is used to host each messaging engine for the Business Process Choreographer bus.

The naming convention for the JDBC data source that the messaging engine uses to interact with the database is:

- System bus: *<node><server>|<cluster>*-SCA.SYSTEM.*<cell>*.Bus
- Application bus: *<node><server>|<cluster>*-SCA.APPLICATION.*<cell>*.Bus
- Common Event Infrastructure: *<node><server>|<cluster>*-CEI.*cellName*.BUS
- Business Process Choreographer bus: *<node><server>*.-BPC.*<cell>*.Bus

The Derby database naming convention is shown below:

- System bus: *install_root*/profiles/*profilename*/databases/com.ibm.ws.sib/ (*<node>.<server>|<cluster>*)-SCA.SYSTEM.*<cell>*.Bus
- Application bus: *install_root*/profiles/*profilename*/databases/com.ibm.ws.sib/ (*<node>.<server>|<cluster>*)-SCA.APPLICATION.*<cell>*.Bus
- Common Event Infrastructure: *install_root*/profiles/*profilename*/event/ DerbyEventBusDB/(*<node>.<server>|<cluster>*)-CEI.*cellName*.BUS
- Business Process Choreographer bus: *install_root*/profiles/*profilename*/databases/ com.ibm.ws.sib/(*<node>.<server>|<cluster>*)-BPC.*<cell>*.Bus

The default for *<cell>* can be the cell name in most cases. However, when a stand-alone profile is federated (only allowed when it is the first node of the cell) then *<cell>* can be the name of that stand-alone profile. You can override this with your own bus identifier name for SCA (not for BPC and CEI). Use [SCA} admin tasks in the scripting client (wsadmin) to create customized names. You cannot use the administrative console to create customized names.

Configuration actions during profile creation

Stand-alone profile

The default messaging engine database for a stand-alone server is Derby Embedded or Derby Embedded 40. You can choose to use a file store for the messaging engine database or you can use another supported database. During profile creation using the Profile Management Tool, you can use the Common database for all messaging engines.

Network deployment

No messaging engine databases are created automatically.

After the profile is created, you can configure a server or a cluster for the Service Component Architecture using the guided activity: Configure your Network Deployment Environment. Access this guided activity from the administrative console of the deployment manager by expanding Guided Activities and clicking Configure your Network Deployment Environment.

You can view the SCA configuration of your server from the Application servers > *servername* > Service Component Architecture panel of the administrative console.

The following administrative tasks are performed during profile creation:
- Remote Destination Location:
  - configSCAAsyncForServer, configSCAJMSForServer (remoteMELocation is true)
  - configSCAAsyncForCluster, configSCAJMSForCluster (remoteMELocation is true)
- Local Destination Location:
  - configSCAAsyncForServer, configSCAJMSForServer
  - configSCAAsyncForCluster, configSCAJMSForCluster

Details of the use of these tasks can be found in "configSCAAsyncForCluster command" and "configSCAAsyncForServer command."

Performing asynchronous SCA configuration for a server or cluster causes a messaging engine to be created for the SCA system bus. Performing the JMS element of the SCA configuration for a server or cluster causes a messaging engine to be created for the SCA application bus. Both the messaging engines require a database or schema to be created.

The Business Process Choreographer messaging engines are created during Business Process Choreographer configuration. Business Process Choreographer is only configured for patterned deployment environments. See "Planning the topology, setup, and configuration path" for more information.

For Common Event Infrastructure messaging engine configuration use `deployEventService` administrative task to configure the event server and the Common Event Infrastructure bus.

SQL scripts

No SQL scripts are created as part of the product. You can use existing base WebSphere Application Server scripts to create database and tables if necessary. The MEDB must be created manually before it is configured using the Application servers > servername > Service Component Architecture panel of the administrative console.

JDBC provider

Service Component Architecture

The JDBC provider is reused when the JDBC provider implementation class has to match with the one chosen in the advanced configuration. This usually means that if the same database types are used, then the implementation classes usually match. If no matching JDBC provider is found in the `resource.xml` file, then the `jdbc-resource-provider-templates.xml` file under `templates/system` (profiles configuration) is searched for a matching JDBC provider. The provider is matched also against the implementation class.

Business Process Choreographer

The Business Process Choreographer reuses the Service Component Architecture messaging engine's JDBC provider. See Configuring Business Process Choreographer for more details.

Common Event Infrastructure

The JDBC provider creation for messaging engine database is similar to the approach followed in the creation of the CEIDB database.

Data source names:
- System bus: : _(*node.server*|*cluster*)-SCA.SYSTEM.*cell*.Bus/*cel/cluster/server/node*
- Application bus: _(*node.server*|*cluster*)-SCA.APPLICATION.*cell*.Bus/*cell/cluster/server/node*
- Common Event Infrastructure: _(*node.server*| *cluster*-CEI.*cellName*.BUS/*cluster/server/node*
- Business Process Choreographer:_(*node.server*|*cluster*)-BPC.*cell*.Bus/*cell/cluster/server/node*

Data source JNDI names:
- System bus: jdbc/com.ibm.ws.sib/(*node.server*|*cluster*)-SCA.SYSTEM.*cell*.Bus/*cell/cluster/server/node*
- Application bus: jdbc/com.ibm.ws.sib/(*node.server*|*cluster*)-SCA.APPLICATION.*cell*.Bus/*cell/cluster/server/node*
- Common Event Infrastructure: Jdbc/ com.ibm.ws.sib /(*node.server*|*cluster*)-CEI.*cellName*.BUS/*cluster/server/node*
- Business Process Choreographer bus: jdbc/com.ibm.ws.sib/(*node.server*|*cluster*)-BPC.*cell*.Bus/*cell/cluster/server/node*

Restrictions

There are no known restrictions.

Tables

For information on the tables, see the topic "Data stores" in the WebSphere Application Server Network Deployment information center.

Exported scripts

The **sibDDLGenerator** script in `WAS_INSTALL_ROOT/bin` can be used to create the SQL scripts for messaging engines database. Use the **sibDDLGenerator** script for creating SQL scripts for use in production environment especially on z/OS platform. See the "The sibDDLGenerator command" for more information.

These scripts only contain basic create `database/tablespace/table` statements. A database administrator may still need to tailor these scripts to meet their database needs, especially on z/OS.

Configuring messaging engine and server behavior when a data store connection is lost

You can determine the behavior of your system when the connection between a running messaging engine and its data store is lost, either due to a failure or because you stop the database for maintenance, through a custom property on the messaging engine.

Setting the `sib.msgstore.jdbcFailoverOnDBConnectionLoss` custom property can enhance the automatic recovery of a highly available WebSphere Process Server environment.

For details on the `sib.msgstore.jdbcFailoverOnDBConnectionLoss` property, including information how to set this property, see *Configuring messaging engine and server behavior when a data store connection is lost* in the WebSphere Application Server information center.

Related information

Configuring messaging engine and server behavior when a data store connection is lost

Enterprise service bus logger mediation database configurations

Use the enterprise service bus logger mediation database specifications for locating information about supported database types; script names and their locations; profile creation configuration actions; schema upgrades and user ID privileges.

The enterprise service bus logger mediation database is used by the MessageLogger mediation primitive in WebSphere Process Server. The Message Logger primitives stores message information in the Common database. The Common database is the default for the enterprise service bus logger mediation database, but you can use an external database. During the profile augmentation phase, the system creates a variable called *ESB_MESSAGE_LOGGER_QUALIFIER* which is set to the value of the chosen Common database schema qualifier.

The database is created automatically for a stand-alone configuration. A set of DDL files are provided to allow you to use additional databases either in a stand-alone server configuration or for a network deployment environment.

For a stand-alone configuration using a DB2 for z/OS database, or for a managed node or deployment manager in a Network Deployment configuration, you must create the Enterprise Service Bus database and storage groups before running the WebSphere Process Server for z/OS configuration script.

Supported database types

The enterprise service bus logger mediation database can use the following database products:

Table 174. Supported database products

Database Types	Considerations
Derby Embedded or Derby Embedded 40	Used as the default database type for standalone profile.
Derby Network Server or Derby Network Server 40	Used as the default database type in network deployment environment.

Table 174. Supported database products (continued)

Database Types	Considerations
DB2 Universal	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 Data Server	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 for z/OS v8 DB2 for z/OS v9	**Important:** When creating a profile for a server that uses DB2 for z/OS v9, the server must be able to connect to the DB2 database.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 UDB for iSeries (Toolbox) DB2 for i5/OS (Toolbox)	Used as a remote database for network deployment environment or as a local database for a standalone profile.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
Informix Dynamic Server	
Microsoft SQL Server (DataDirect)	
Microsoft SQL Server (Microsoft)	
Oracle	You need sysdba privilege to create the database, tables and schemas. Failure to have the correct sysdba privilege can result in errors creating and accessing the tables and schemas.

User ID privileges

The user credentials that you provide in the Profile Management Tool must have the permissions necessary to create table spaces, tables, schemas, indexes, and stored procedures. For the Create new database option, the user identity must have the necessary privileges to create a new database. See "Users and schemas for databases" and "Database privileges" for more information.

Note: If the user running the script has enough authority to create tables, the script will not require an authentication ID within the script.

Database Management Service (DBMS) instances

The Common database is used for both the standalone and network deployment environments at cell scope. However, users can manually create as many other instances as they require (each message logger mediation primitive can be configured to use a different data source and hence a different database).

Configuration actions during profile creation

For the standalone and deployment manager profiles the enterprise service bus logger profile will execute the Common database script **createTable** in the Common database. See the"Common database specifications" for more information.

Stand-alone profile

In a default stand-alone environment a Derby database is automatically created named EsbLogMedDB.

Network deployment environment

The default enterprise service bus database is not automatically selected during network deployment profile creation. You must chose either the default database or one of the supported databases.

SQL scripts

The SQL script **createTable_ESB.sql** is located in *install_root*/dbscripts/ CommonDB/*DBTYPE*.

The scripts **createMessageLoggerResource.jacl** and **removeMessageLoggerResource.jacl** are located in *install_root*/bin and can be used to create or delete tables in the requested database type.

JDBC provider

The Common database JDBC provider and data source are used by default:

Data source name:
- WPS DataSource

Data source JNDI name:
- jdbc/WPSDB

You can create your own data source configuring the Message Logger mediation to use a different data source.

Restrictions

There are no known restrictions.

Tables

The enterprise service bus logger mediation database uses the MSGLOG table in the Common database. You can choose not to use the Common database, and you can use an external database if desired.

Exported scripts

The database scripts are exported to the following location: *install_root*/ dbscripts/CommonDB/*DBTYPE*/*dbName*

Schema upgrade scripts

No schema upgrade involved for MSGLOG table. When you migrate to WebSphere Process Server version 6.1, WebSphere Process Server continues to use the **MessageLogger** databases used in prior releases. There is no support to migrate this data into the WebSphere Process Server Common database.

If you want to maintain a single location for message information, you can
*   Manually move the data from the old database to the new database
*   Continue to use the old database
*   Use the createMessageLoggerResource.jacl script to move the data.

Selector and business rules group database configurations

Use the Selector and business rules group database specifications to find information about supported database types; scripts and their locations; profile creation configuration actions; restrictions; table names; and user ID privileges.

When you install an application containing selector or business rule artifacts, the server stores these artifacts in database tables so that you can dynamically update them without changing the application. The selector and business rules group components use a database to hold the selector and business rule artifacts that are created in WebSphere Integration Developer and installed on the server. If you make any changes to a selector through the administrative console or to business rules through the business rules manager, the database is updated with the latest information. The original artifacts in the EAR are not synchronized with any updates made after the application is installed.

Supported database types

The selector and business rules group database can use the following database products:

Table 175. Supported database products

Database Types	Considerations
Derby Embedded or Derby Embedded 40	Used as the default database type for standalone profile.
Derby Network Server or Derby Network Server 40	Used as the default database type in network deployment environment.
DB2 Universal	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 Data Server	Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
DB2 for z/OS v8 DB2 for z/OS v9	**Important:** When creating a profile for a server that uses DB2 for z/OS v9, the server must be able to connect to the DB2 database.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.

Table 175. Supported database products (continued)

Database Types	Considerations
DB2 UDB for iSeries (Toolbox) DB2 for i5/OS (Toolbox)	Used as a remote database for network deployment environment or as a local database for a standalone profile.Used as the database in network deployment configurations. Optionally, can be used as the database in stand-alone server configurations.
Informix Dynamic Server	
Microsoft SQL Server (DataDirect)	
Microsoft SQL Server (Microsoft)	
Oracle	You need sysdba privilege to create the database, tables and schemas. Failure to have the correct sysdba privilege can result in errors creating and accessing the tables and schemas.

User ID privileges

The user credentials that you provide in the Profile Management Tool must have the permissions necessary to create table spaces, tables, schemas, indexes, and stored procedures. For the Create new database option, the user identity must have the necessary privileges to create a new database. See "Users and schemas for databases" and "Database privileges" for more information.

Note: If the user running the script has enough authority to create tables, the script will not require an authentication ID within the script.

Database Management Service (DBMS) instances

Only one database instance is available in a stand-alone profile or network deployment configuration (server or cluster of servers). All selectors and business rules for the server in a stand-alone profile or in a cell use the same repository. There is no support for using separate database instances for different selectors or business rules.

Configuration actions during profile creation

Stand-alone profile

During profile creation, the Common database uses createTable to create Business Rules and Selector tables. If you choose the default configuration, the default database is Derby Embedded or Derby Embedded 40. However, you cannot use multiple servers because Derby Embedded or Derby Embedded 40 allows only one Java virtual machine to access the database at a time.

Deployment manager profile

For network deployment configuration, the Common database for the cell is set up with the appropriate tables for selector and business rule group components. All selectors and business rules for the server in a deployment manager or custom profile will use this database.

SQL scripts

See the Common database specifications for SQL script locations.

JDBC provider

The Selectors and Business Rules uses the Common database data source and JBDC provider:

Data source name:
- `WPS DataSource`

Data source JNDI name:
- `jdbc/WPSDB`

Restrictions

When applications that contain selectors or business rules are uninstalled from the server or cell, the artifacts stored in the Common database or RepositoryDB databases are not removed. These must be removed manually following the instructions in the topic: "Removing business rule and selector data from the repository."

When you uninstall applications which contain Selectors or Business Rules from a server or cell, the artifacts stored in the Common database are not removed. These must be removed manually per the instructions in the Information Center: "Removing business rule and selector data from the repository."

Tables

For selectors and business rule groups, there are three tables which are used to hold the artifacts:
- ByteStore
- ByteStoreOverflow
- AppTimestamp

Exported scripts

The scripts are exported to the same location as the scripts for the Common database, except when using Derby Embedded or Derby Embedded 40, where no scripts are exported. See the "Common database specifications" for script locations.

Creating the database design file using the database design tool

Use the database design tool (DDT) to generate a design file that is used to create the database tables required by WebSphere Process Server. The DDT generates the design file from a user specified properties file or user interactive input. The resulting design file is then used by the DDT to create the database scripts that are used to create the database tables. Additionally, the design file can be used as input during profile creation and during deployment environment configuration to specify the database configuration properties.

Before you begin

You must have a list of all database requirements and schema names. See
"Prerequisites for creating or augmenting profiles" on page 189.

About this task

The following steps describe how to use the DDT to generate the design file and
database scripts. The input for the DDT is either a user specified properties file or
user interactive input.

The **DbDesignGenerator** command has the following options.

```
-? , -help
   display help info.

-e db_design_file_name
   edit the specified database design file (e.g. *.dbDesign, *.properties).

-v db_design_file | db_scripts_output_directory
   when a db_design_file is given, validation will be done on the specified
 database design file based on the database specs.
When a db_scripts_output_directory is given, the database scripts
in the specified directory will be validated. Currently only
scripts generated from template ddl generator can be validated.

-g db_design_file [-d output_directory] [db_design_file2] [-d output_directory2] ...
[db_design_fileN] [-d output_directoryN]
   generate the database scripts from the specified design files in batch mode.
The generated scripts will be put in the corresponding output
directories or the default locations if output directories are absent.
```

Note: The DDT does not support the generation of database scripts for Common
Event Infrastructure.

Note: The following restrictions apply to stand-alone database design for Common
Event Infrastructure components.

Table 176. Stand-alone Database design restrictions for CEI component:

Database type	CEI restrictions
DB2 Distributed	The database name must not be the same as the commonDB name. Edit the CEI database design and choose a different name.
SQL Server	• dbServerName cannot be empty. Edit the CEI database design and provide the database server name. • dbUser cannot be the same as the CommonDB user ID. Edit the CEI database design and provide a different user ID. • sysUser and sysPassword cannot be empty. Edit the CEI database design and provide the system user ID and system password.

Table 176. Stand-alone Database design restrictions for CEI component: (continued)

Database type	CEI restrictions
Oracle	• dbUser cannot be the same as the CommonDB user ID. Edit the CEI database design and provide a different user ID. • sysUser and sysPassword cannot be empty. Edit the CEI database design and provide the system user ID and system password.

Procedure

1. Generate the design file and database scripts using the **DbDesignGenerator** command, which is located in:

   install_root\util\dbUtils

   /*install_root*/util/dbUtils

   ```
   DbDesignGenerator.bat - for Windows
   DbDesignGenerator.sh - for Unix and z/OS
   ```

   Returns the main menu:

   ```
   [info] running DbDesignGenerator in interactive mode...

   [info] Enter 'q' to quit without saving; '-' for back to previous
   menu; '?' for help at any time.
   [info] To accept the given default values, simply press the 'Enter' key.[info]
   Please pick one of the following [design option(s)] :
   ```
   ```
   (1)Create a database design for Standalone profile or Deployment
   Environment
   (2)Create a database design for a single component (e.g. BPC, CEI etc)
   (3)Edit an existing database design
   (4)Generate database scripts from a database design
   (5)exit [q]
   ```

2. Refer to 3 on page 32 in "Creating the Common database manually before product installation" on page 31 for steps on running the database scripts.

   Note: See "Database design tool examples" for usage examples.

Related tasks

"Creating a deployment environment definition using the command line" on page 462
You can create a deployment environment definition using the wsadmin command.
Running createDeploymentEnvDef provides the definition of the deployment environment.

Database design tool examples

These examples demonstrate how to use the database design tool to generate the design file by database type.

For all database types

When you generate scripts using the dbDesign file, you will receive the following warning message. The CEI scripts will have to be generated separately.

```
generate database scripts? (y/n) [default=y] :y
```

```
[warning] database scripts generation failed for [WBI_CEI_EVENT] due to DDL provider is
not available. You will not be able to generate SQL scripts for the component: CEI
```

DERBY EMBEDDED

If you select wps.standalone as the database pattern and Derby Embedded as the default database when using the DbDesignGenerator command in interactive mode, you must manually configure the business space authentication properties for BSpace.WBI_BSPACE.

Note: If you select wps.nd.topology as the database pattern, you will not be able to select Derby Embedded. You will need to select Derby Network Server instead.

```
[info] Please edit any database component with status of 'not complete' for required prope
rties.
[info] Completed database components can be edited to change existing or defaulted propert
y values.
[info] Design the 'master' component first, and then any parent components, since other co
mponents may inherit values from them.

[info] Please pick one of the following [database component(s)] :

(1)[CommonDB]    WBI_CommonDB : [master] [status = complete]
(2)[BPCReporting]       WBI_BPCEventCollector :  [status = complete]
(3)[BPC]        WBI_BPC :  [status = complete]
(4)[BSpace]     WBI_BSPACE :  [status = not complete]
(5)[CEI]        WBI_CEI_EVENT :  [status = complete]
(6)[SibME]      WBI_SCA_SYS_ME :  [status = complete]
(7)[SibME]      WBI_BPC_ME : [parent = WBI_SCA_SYS_ME] [status = complete]
(8)[SibME]      WBI_CEI_ME : [parent = WBI_SCA_SYS_ME] [status = complete]
(9)[SibME]      WBI_SCA_APP_ME : [parent = WBI_SCA_SYS_ME] [status = complete]
(10)[save and exit]

Please enter the number for the database component :4

--------------------------------------------------------------------------------

[status] WBI_BSPACE is not complete with 2 remaining item(s):
[ 1 ] BSpace.WBI_BSPACE : authAlias : required property 'userName' for userId is empty.
[ 2 ] BSpace.WBI_BSPACE : authAlias : required property 'password' for DB_PASSWORD
is empty.

Edit this database component? (y/n) [default=y] :



b) For DbDesignGenerator under interactive mode, when user selects to generate wps.nd.
topology, user should not be able to select Derby Embedded as default db. (But this option hasn't
been taken out just yet, so we should let the user know not to select it)

[status] WBI_CommonDB is not complete with 1 remaining item(s):
[ 1 ] CommonDB.WBI_CommonDB :  : DbType key is not set.

Edit this database component? (y/n) [default=y] :

[info] Please pick one of the following [database type(s)] :

(1)DB2-distributed
(2)DB2-iSeries
(3)DB2-zOS-8
(4)DB2-zOS-9
(5)Derby-embedded
(6)Derby-networkServer
(7)Informix
(8)Oracle
(9)SQL Server
```

INFORMIX

If you select wps.standalone or wps.nd.topology, after configuring the
CommonDB, you must manually configure both BPCReporting and business space
because the Informix database type is not supported for these data sources.

```
[info] Please pick one of the following [database component(s)] :

(1)[CommonDB]    WBI_CommonDB : [master] [status = complete]
(2)[BPCReporting]       WBI_BPCEventCollector :  [status = not complete]
(3)[BPC]         WBI_BPC :  [status = complete]
(4)[BSpace]      WBI_BSPACE :  [status = not complete]
(5)[CEI]         WBI_CEI_EVENT :  [status = complete]
(6)[SibMe]       WBI_BPC_ME : [parent = WBI_CommonDB] [status = complete]
(7)[SibMe]       WBI_CEI_ME : [parent = WBI_CommonDB] [status = complete]
(8)[SibMe]       WBI_SCA_APP_ME : [parent = WBI_CommonDB] [status = complete]
(9)[SibMe]       WBI_SCA_SYS_ME : [parent = WBI_CommonDB] [status = complete]
(10)[save and exit]

Please enter the number for the database component :4

-------------------------------------------------------------------------------

[status] WBI_BSPACE is not complete with 1 remaining item(s):
[ 1 ] BSpace.WBI_BSPACE :  : DbType key is not set.

Edit this database component? (y/n) [default=y] :
```

ORACLE

If you select wps.standalone or wps.nd.topology, after configuring the
CommonDB, you must manually configure business space for the required
database authentication.

```
[info] Please pick one of the following [database component(s)] :

(1)[CommonDB]    WBI_CommonDB : [master] [status = complete]
(2)[BPCReporting]       WBI_BPCEventCollector :  [status = complete]
(3)[BPC]         WBI_BPC :  [status = complete]
(4)[BSpace]      WBI_BSPACE :  [status = not complete]
(5)[CEI]         WBI_CEI_EVENT :  [status = complete]
(6)[SibMe]       WBI_BPC_ME : [parent = WBI_CommonDB] [status = complete]
(7)[SibMe]       WBI_CEI_ME : [parent = WBI_CommonDB] [status = complete]
(8)[SibMe]       WBI_SCA_APP_ME : [parent = WBI_CommonDB] [status = complete]
(9)[SibMe]       WBI_SCA_SYS_ME : [parent = WBI_CommonDB] [status = complete]
(10)[save and exit]

Please enter the number for the database component :4

-------------------------------------------------------------------------------

[status] WBI_BSPACE is not complete with 3 remaining item(s):
[ 1 ] BSpace.WBI_BSPACE : databaseObjects : required property 'databaseUser' for DB_USER i
s empty.
[ 2 ] BSpace.WBI_BSPACE : authAlias : required property 'userName' for userId is empty.
[ 3 ] BSpace.WBI_BSPACE : authAlias : required property 'password' for DB_PASSWORD is empt
y.

Edit this database component? (y/n) [default=y] :
```

SQL Server

If you select wps.standalone or wps.nd.topology, after configuring the
CommonDB, you must manually configure BPCReporting because SQL Server is
not supported for that data source.

```
[info] Please pick one of the following [database component(s)] :

(1)[CommonDB]   WBI_CommonDB : [master] [status = complete]
(2)[BPCReporting]       WBI_BPCEventCollector :  [status = not complete]
(3)[BPC]        WBI_BPC :  [status = complete]
(4)[BSpace]     WBI_BSPACE :  [status = complete]
(5)[CEI]        WBI_CEI_EVENT :  [status = complete]
(6)[SibMe]      WBI_BPC_ME : [parent = WBI_CommonDB] [status = complete]
(7)[SibMe]      WBI_CEI_ME : [parent = WBI_CommonDB] [status = complete]
(8)[SibMe]      WBI_SCA_APP_ME : [parent = WBI_CommonDB] [status = complete]
(9)[SibMe]      WBI_SCA_SYS_ME : [parent = WBI_CommonDB] [status = complete]
(10)[save and exit]

Please enter the number for the database component :2

------------------------------------------------------------------------------

[status] WBI_BPCEventCollector is not complete with 1 remaining item(s):
[ 1 ] BPCReporting.WBI_BPCEventCollector :  : DbType key is not set.

Edit this database component? (y/n) [default=y] :
```

DB2-iSeries

If you select wps.standalone or wps.nd.topology, after configuring the CommonDB, you must manually configure BPCReporting, BPC, and CEI for the OS400_TOOLBOX_JDBC_DRIVER_PATH parameter.

```
[info] Please pick one of the following [database component(s)] :

(1)[CommonDB]   WBI_CommonDB : [master] [status = complete]
(2)[BPCReporting]       WBI_BPCEventCollector :  [status = not complete]
(3)[BPC]        WBI_BPC :  [status = not complete]
(4)[BSpace]     WBI_BSPACE :  [status = complete]
(5)[CEI]        WBI_CEI_EVENT :  [status = not complete]
(6)[SibMe]      WBI_BPC_ME : [parent = WBI_CommonDB] [status = complete]
(7)[SibMe]      WBI_CEI_ME : [parent = WBI_CommonDB] [status = complete]
(8)[SibMe]      WBI_SCA_APP_ME : [parent = WBI_CommonDB] [status = complete]
(9)[SibMe]      WBI_SCA_SYS_ME : [parent = WBI_CommonDB] [status = complete]
(10)[save and exit]

------------------------------------------------------------------------------

[status] WBI_BPCEventCollector is not complete with 1 remaining item(s):
[ 1 ] BPCReporting.WBI_BPCEventCollector : variables : required property 'os400toolbox_jd
c_driver_path' for OS400_TOOLBOX_JDBC_DRIVER_PATH is empty.

------------------------------------------------------------------------------

[status] WBI_BPC is not complete with 1 remaining item(s):
[ 1 ] BPC.WBI_BPC : variables : required property 'os400toolbox_jdbc_driver_path' for OS4
0_TOOLBOX_JDBC_DRIVER_PATH is empty.

------------------------------------------------------------------------------

[status] WBI_CEI_EVENT is not complete with 1 remaining item(s):
[ 1 ] CEI.WBI_CEI_EVENT : variables : required property 'os400toolbox_jdbc_driver_path' f
r OS400_TOOLBOX_JDBC_DRIVER_PATH is empty.
```

DB2-zOS8/zOS9

If you select wps.standalone or wps.nd.topology, after configuring the CommonDB, you must manually configure business space for the dbConnectionLocation parameter.

```
[info] Please pick one of the following [database component(s)] :

(1)[CommonDB]     WBI_CommonDB : [master] [status = complete]
(2)[BPCReporting]        WBI_BPCEventCollector :  [status = complete]
(3)[BPC]          WBI_BPC :  [status = complete]
(4)[BSpace]      WBI_BSPACE :  [status = not complete]
(5)[CEI]          WBI_CEI_EVENT :  [status = complete]
(6)[SibMe]        WBI_BPC_ME : [parent = WBI_CommonDB] [status = complete]
(7)[SibMe]        WBI_CEI_ME : [parent = WBI_CommonDB] [status = complete]
(8)[SibMe]        WBI_SCA_APP_ME : [parent = WBI_CommonDB] [status = complete]
(9)[SibMe]        WBI_SCA_SYS_ME : [parent = WBI_CommonDB] [status = complete]
(10)[save and exit]

Please enter the number for the database component :4

-------------------------------------------------------------------------------

[status] WBI_BSPACE is not complete with 1 remaining item(s):
[ 1 ] BSpace.WBI_BSPACE : databaseObjects : required property 'dbConnectionLocation' for D
B_CONNECTLOCATION is empty.
```

Database design tool troubleshooting

DDT troubleshooting information, includes diagnostic and validation information
that you can use to diagnose problems that occur in the database scripts.

Required property is empty errors

The following messages will be returned when the required userName and password
properties are not set.

```
[status] WBI_BSPACE is not complete with 2 remaining item(s):
[ 1 ] BSpace.WBI_BSPACE : authAlias : required property 'userName' for userId is empty.
[ 2 ] BSpace.WBI_BSPACE : authAlias : required property 'password' for DB_PASSWORD is empty.
```

Sample output of running a validation of the existing database design

```
DbDesignGenerator.bat -v DB2-distributed-
...
[WARNING] 2 potential problems are found in the scripts. They are
DB_USER @ line 46 in file configCommonDB.bat
DB_USER @ line 80 in file configCommonDB.sh
```

Additional database configuration information

The topics in this section provide additional database configuration information for
WebSphere Process Server.

Users and schemas for databases

During the installation of WebSphere Process Server, you have the option of using
the default schema name and user ID privileges when installing your databases.
However, your database design may require separate user ID and schema name
privileges. You can review the three provided scenarios to determine when and
how to configure different schema name and user ID privileges when installing
WebSphere Process Server.

Single user ID or schema name privileges for default configuration

If you chose a default installation for your databases, WebSphere Process Server
requires a minimum of one user ID or schema name with the ability to create
tables and to select, insert, update, and delete rows in those tables. You can use
Profile Management Tool or Installer to create your databases. Table 177 on page
438

438 shows the default database configuration properties using DB2 as your database vendor. Other database vendors have different default database configuration properties.

Table 177. Default user ID and schema name privileges using DB2

Database tables	Default database name with DB2	User ID or schema name
Common database tables	WPRCSDB	WebSphere Process Server provides a user ID during installation
Business Process Choreographer	BPEDB	WebSphere Process Server provides a user ID during installation
Messaging tables	MEDB	WebSphere Process Server provides a schema name during installation

Multiple user ID or schema name privileges

If your database design has different properties, you may need multiple user ID and schema name privileges. Provided are three scenarios along with tables to show you how to apply the configuration to achieve your desired design. If your particular design is not in the three provided scenarios, a review of these scenarios should help you implement your particular design.

Scenario 1

In this scenario you use a schema name that is the same as the user ID privileges, but you are not using the default schema name or user ID privileges. This single user ID can access all the database and also create all needed tables. The following are examples of scenario 1 privileges:

- Schema name: dog
- Schema name for SCA.SYSTEM ME : dogSYS
- Schema name for SCA.APP ME: dogAPP
- Schema name for Event ME: dogEvent
- Schema name for BPC ME: dogBPC
- User ID to create schemas: dog
- User ID to select, insert, update, and delete schemas: dog

Table 178 on page 439 is a list of how to set up the schema name and user ID privileges using DB2 as your database vendor. If you choose a different databases vendor, see their documentation for setting up schema names and user ID privileges.

Table 178. Scenario 1

Database tables	Database name with DB2	Schema name	User ID to create tables	User ID to select, insert, update, and delete rows
Common database tables	You supply this value in the • Installation wizard • Profile Management Tool • Silent install • Silent profile creation	This schema name is the same as the user ID used to select, insert, update, and delete rows.	This value is the same as the user ID used to select, insert, update, and delete rows.	You supply this value in the • Installation wizard • Profile Management Tool • Silent install • Silent profile creation
Business Process Choreographer tables	You supply this value twice: 1. In table creation scripts 2. While configuring a deployment target using one of the following: • Administrative console • Installation wizard • bpeconfig.jacl	This schema name is the same as the user ID used to select, insert, update, and delete rows.	This value is the same as the user ID used to select, insert, update, and delete rows.	You supply this value twice: 1. In table creation scripts 2. While configuring a deployment target using one of the following: • Administrative console • Installation wizard • bpeconfig.jacl

Scenario 2

In this scenario you use the same the schema name and user ID to select, insert, update, and delete schemas. However, you use a different user ID to create the schemas. The following are examples of scenario 2 privileges:

• Schema name: snow
• Schema name for SCA.SYSTEM ME: snowSYS
• Schema name for SCA.APP ME: snowAPP
• Schema name for Event ME: snowEvent
• Schema name for BPC ME: snowBPC
• User ID to create the schemas: rock
• User ID to select, insert, update, and delete schemas: snow

Table 179 on page 440 is a list of how to set up the schema name and user ID privileges using DB2 as your database vendor. If you choose a different databases vendor, see their documentation for setting up schema names and user ID privileges.

Table 179. Scenario 2

Database tables	Database name with DB2	Schema name	User ID to create tables	User ID to select, insert, update, and delete rows
Common database tables	You supply this value twice: 1. In table creation scripts 2. During the WebSphere Process Server configuration using one of the following: • Administrative console • Installation wizard • Profile Management Tool • Silent install • Silent profile creation • bpeconfig.jacl **Note:** If you execute the Installer first, then you supply the value once because the generated scripts already contain the correct schema name and user ID values.	The table creation scripts need to be modified with the schema name that allows reading and writing rows.	The table creation script needs to be modified with the user ID that allows table creation.	You supply the user ID during profile creation through one of the following: • Installation wizard • Profile Management Tool • Silent install • Silent profile creation
Business Process Choreographer tables	You supply this value twice: 1. In table creation scripts 2. While configuring a deployment target using one of the following: • Administrative console • Installation wizard • bpeconfig.jacl	The table creation scripts need to be modified with the schema name that allows reading and writing rows.	The table creation script needs to be modified with the user ID that allows table creation.	You supply the user ID during profile creation through one of the following: • Installation wizard • Profile Management Tool • Silent install • Silent profile creation

Scenario 3

In this scenario you use the same user ID to create all schemas. However, each schema has a different user ID to select, insert, update, and delete rows. The following are examples of scenario 3 privileges:

- Schema name: waterCom
- Schema name for common tables: waterCom
- Schema name for SCA.SYSTEM ME: waterSYSME
- Schema name for SCA.APP ME: waterAPPME
- Schema name for Event ME: waterEventME

- Schema name for BPC ME: waterBPCME
- Schema name for BPC and HTM tables: waterBPC
- Schema name for ESBMessaging tables: waterESB
- User ID to create schemas: milk
- User ID to select, insert, update, and delete schemas:

Schema name	User ID to select, insert, update, and delete schemas
waterCom	waterCom
waterSYSME	waterSYSME
waterAPPME	waterAPPME
waterEventME	waterEventME
waterBPCME	waterBPCME
waterBPC	waterBPC
waterESB	waterESB

Table 180 is a list of how to set up the schema name and user ID privileges using DB2 as your database vendor. If you choose a different databases vendor, see their documentation for setting up schema names and user ID privileges.

Table 180. Scenario 3

Database tables	Database name with DB2	Schema name	User ID to create tables	User ID to select, insert, update, and delete rows
Common database tables	You supply this value in the • Installation wizard • Profile Management Tool • Silent install • Silent profile creation	This schema name is the same as the user ID used to select, insert, update, and delete rows.	This value is the same as the user ID used to select, insert, update, and delete rows.	You supply the user ID during profile creation through one of the following: • Installation wizard • Profile Management Tool • Silent install • Silent profile creation

Business Process Choreographer tables	You supply this value twice:
	1. In table creation scripts
	2. While configuring a deployment target using one of the following:
	  • Administrative console
	  • Installation wizard
	  • bpeconfig.jacl
		The table creation scripts need to be modified with a schema name that is used to select, insert, update, and delete rows.	This value is the same as the user ID used to select, insert, update, and delete rows.	You supply this value twice:
				1. In table creation scripts
				2. While configuring a deployment target using one of the following:
				  • Administrative console
				  • Installation wizard
				  • bpeconfig.jacl

Table 180. Scenario 3 (continued)

Database tables	Database name with DB2	Schema name	User ID to create tables	User ID to select, insert, update, and delete rows
Messaging tables	You supply this value with the definition of each messaging engine.	The table creation scripts need to include the schema name that is used to select, insert, update, and delete rows.	This value is the same as the user ID used to select, insert, update, and delete rows.	You supply this value during the creation of the messaging engine. Select the create table option during the messaging engine configuration.

JDBC providers

You can use JDBC providers to interact applications with relational databases.

Applications use JDBC providers to interact with relational databases. The JDBC provider supplies the specific JDBC driver implementation class for access to a specific type of database. To create a pool of connections to that database, you associate a data source with the JDBC provider. Together, the JDBC provider and the data source objects are functionally equivalent to the Java EE Connector Architecture (JCA) connection factory, which provides connectivity with a non-relational database.

Refer to the examples of both Typical stand-alone environment setup and Typical deployment environment setup in the previous topic.

For more information on JDBC providers, see "JDBC providers" in the WebSphere Application Server information center.

Data sources

Data sources provide the link between applications and relational databases.

Applications use a data source to obtain connections to a relational database. A data source is analogous to the Java EE Connector Architecture (JCA) connection factory, which provides connectivity to other types of enterprise information systems (EIS).

A data source is associated with a JDBC provider, which supplies the driver implementation classes that are required for JDBC connectivity with a specific type of database. Application components transact directly with the data source to obtain connection instances to your database. The connection pool that corresponds to each data source provides connection management.

You can create multiple data sources with different settings, and associate them with the same JDBC provider. For example, you might use multiple data sources to access different databases within the same database application. WebSphere Process Server requires JDBC providers to implement one or both of the following data source interfaces, which are defined by Sun Microsystems. These interfaces enable the application to run in a single-phase or two-phase transaction protocol.

Note: Business Process Choreographer data sources are created using the Business Process Choreographer configuration tools. Refer to Configuring Business Process Choreographer.

• ConnectionPoolDataSource - a data source that supports application participation in local and global transactions, except two-phase commit transactions. When a connection pool data source is involved in a global

transaction, transaction recovery is not provided by the transaction manager. The application is responsible for providing the backup recovery process if multiple resource managers are involved.

- XADataSource - a data source that supports application participation in any single-phase or two-phase transaction environment. When this data source is involved in a global transaction, the WebSphere Application Server transaction manager provides transaction recovery.

The following tables provide examples of typical stand-alone and typical deployment environment setups:

Table 181. Typical stand-alone environment setup

Datasource	Component	Scope	JNDI Name
WBI DataSource	CommonDB	Node	jdbc/WPSDB
SCA Application Bus ME data source	SCA ME	Server	jdbc/com.ibm.ws.sib/nlNode01.server1-SCA.APPLICATION.localhostNode01Cell.Bus
Business Process Choreographer data source	BPC	Server	jdbc/BPEDB
Business Process Choreographer ME data source	BPC ME	Server	jdbc/com.ibm.ws.sib/nlNode01.server1-BPC.localhostNode01Cell.Bus
event	CEI	Server	jdbc/cei
CEI ME data source	CEI ME	Server	jdbc/com.ibm.ws.sib/nlNode01.server1-CEI.*cellName*.BUS

Table 182. Typical deployment environment setup

Datasource	Component	Scope	JNDI Name
WBI DataSource	CommonDB	Cell	jdbc/WPSDB
SCA Application Bus ME data source	SCA ME	Cluster	jdbc/com.ibm.ws.sib/clusterone-SCA.APPLICATION.enduranceTestCell01.Bus
Business Process Choreographer data source	BPC	Cluster	jdbc/BPEDB
Business Process Choreographer ME data source	BPC ME	Cluster	jdbc/com.ibm.ws.sib/clusterone-BPC.enduranceTestCell01.Bus
event	CEI	Cluster	jdbc/cei
CEI ME data source	CEI ME	Cluster	jdbc/com.ibm.ws.sib/clusterone-CEI.*cellName*.BUS

For more information on data sources, see "Data sources" in theWebSphere Application Server information center.

Table and schema creation matrices

Use the table and schema creation matrices to determine what database tables and schemas will be created automatically for each database provider if **Create Tables** is enabled.

Purpose

In **Resources > JDBC > Business Integration Data Sources > *Data Source***, you can select the check box for **Create Tables** to allow the component to create the tables the first time it accesses the data source. If your site policy restricts table creation to a database administrator, deselect the check box, locate the scripts in the message box and give these scripts to your database administrator to run. If **Create Tables** is enabled, the following tables show tables and schemas are created for the various deployment environment functions for each database provider. An "X" indicates the table or schema is created.

Note: You configure Common database during profile creation.

Note: The create table flag will be disabled for Common Event Infrastructure after the Common Event Infrastructure database has been configured. The Common Event Infrastructure tables can only be created when the Common Event Infrastructure server is being configured.

Table 183. Table creation based on database provider

Database providers	Messaging Engine	Business Process Choreographer	Business Process Choreographer reporting	Common Event Infrastructure	Mediation Logger
Derby Embedded or Derby Embedded 40	X	X	X	X	
Derby Network Server or Derby Network Server 40	X	X	X	X	
DB2 Universal	X	X	X	X	
• DB2 UDB for iSeries (Toolbox) • DB2 for i5/OS (Toolbox)	X	X	X	X	
• DB2 for z/OS v8 • DB2 for z/OS v9					
Oracle	X	X	X	X	
• Microsoft SQL Server (DataDirect) • Microsoft SQL Server (Microsoft)	X	X		X	
Informix Dynamic Server	X	X		X	

Note: If DB2 UDB for iSeries database is not local, Common Event Infrastructure does not support schema creation. Database creation scripts are generated and then used by Common Event Infrastructure.

Table 184. Schema creation based on by database provider

Database providers	Messaging Engine	Business Process Choreographer	Business Process Choreographer Reporting	Common Event Infrastructure	Mediation Logger
Derby Embedded or Derby Embedded 40	X	X	X	X	

Table 184. Schema creation based on by database provider (continued)

Database providers	Messaging Engine	Business Process Choreographer	Business Process Choreographer Reporting	Common Event Infrastructure	Mediation Logger
Derby Network Server or Derby Network Server 40	X	X	X	X	
DB2 Universal	X	X	X	X	
• DB2 UDB for iSeries (Toolbox) • DB2 for i5/OS (Toolbox)	X	X	X	X	X
• DB2 for z/OS v8 • DB2 for z/OS v9					
Oracle	X	X	X	X	
• Microsoft SQL Server (DataDirect) • Microsoft SQL Server (Microsoft)					
Informix Dynamic Server					

Note: If DB2 UDB for iSeries database is not local, Common Event Infrastructure does not support schema creation. Database creation scripts are generated and then used by Common Event Infrastructure.

Setting up deployment environments

Setting up deployment environments involves creating the deployment environment definition and then generating the environment.

About this task

You can create the deployment environment by using the Deployment Environment configuration wizard or through scripting using wsadmin. When you have finished creating the deployment environment, you can perform additional tasks to complete the deployment environment setup.

You can also create a deployment environment and a custom deployment environment at profile creation time using the Profile Management Tool. For information on choosing how to create your deployment environment, see Planning your deployment environment.

Related tasks

➡ Planning your deployment environment
Setting up your deployment environment involves many decisions that affect
everything from the number of physical servers to the type of pattern you choose.
Each decision will affect how you set up your deployment environment.

"Creating Deployment environment deployment manager profiles" on page 220
Learn how to use the **Deployment environment** option of the Profile Management
Tool to create and configure WebSphere Process Server or WebSphere Enterprise
Service Bus deployment manager profiles. Selecting the **Deployment environment**
option lets you configure a profile with customized configuration values and use it
in a new deployment environment based on a supplied pattern.

"Creating **Deployment environment** custom profiles (managed nodes)" on page
235
Learn how to use the **Deployment environment** option of the Profile Management
Tool to create and configure WebSphere Process Server or WebSphere Enterprise
Service Bus custom profiles. Selecting the **Deployment environment** option lets
you configure a profile with customized configuration values to be used in an
existing deployment environment pattern.

Creating deployment environments

Creating deployment environments involves creating the deployment environment
definition and then generating the environment. You can create deployment
environments using the Deployment Environment Configuration wizard or by
using wsadmin.

The Deployment Environment Configuration wizard presents you with a series of
panels from which you can configure the components and clusters that make up
your deployment environment. When you finish entering information on the
Deployment Environment Configuration wizard panels, and you click **Finish** (but
not **Generate**), the result is a *deployment environment definition*. Only after you click
Generate in the Deployment Environment Configuration wizard is the
environment "configured". When you generate a deployment environment
definition from the Deployment Environment Configuration wizard, the system
configures all the clusters and components based on the data in the generated
definition.

As well as being able to create deployment environments from the Deployment
Environment Configuration wizard, you can also create deployment environments
using wsadmin scripting. As with the Deployment Environment Configuration
wizard, the wsadmin function for creating a deployment environment has two
stages - first you create the deployment environment definition and then you
generate the deployment environment from that definition.

Creating deployment environments using the Deployment Environment configuration wizard

You can create the deployment environment by using the Deployment
Environment configuration wizard.

Creating a deployment environment using a pattern:

After you select a deployment pattern, use the Deployment Environment
Configuration wizard to create the deployment environment that is based on the
pattern.

Before you begin

On the administrative console of the deployment manager navigate to **Servers > Deployment Environments**.

Required security role for this task: When security and role-based authorization are enabled, you must log in to the administrative console as an administrator or configurator to perform this task.

The procedure for creating deployment environments using the deployment environment wizard includes steps for selecting patterns and features, and therefore it is assumed that you have read and understood the information on patterns and features documented in the planning section.

It is assumed that you have installed the product and that you have created the deployment manager profile and the associated nodes.

Additionally, one of the steps in the Deployment Environment Configuration wizard includes importing a database design document. The database design document defines the database configuration for the selected deployment environment features. WebSphere Process Server includes a response-driven database design tool (DDT) that creates a database design document based on user inputs. The document then can be used by the DDT to create the database scripts and by the WebSphere Process Server deployment environment wizard to configure the databases used in the deployment environment. For more information on the DDT and for more information on database configuration in general, see *Configuring databases*.

About this task

This task describes the procedure for creating a deployment environment that is based on a specific pattern and uses the Deployment Environment Configuration wizard.

Note: If you make an error while you are working in the wizard, you can go back by clicking **Back**.

Procedure
1. From the administrative console, go to the Deployment Environments page by clicking **Servers ▸ Deployment Environments** .
2. Launch the Deployment Environment Configuration wizard by clicking **New** on the Deployment Environments page.
   a. The **Create a deployment environment based on a pattern** option is selected. **Create a deployment environment based on a pattern** is the system default and it is the option described in this topic.

      Deployment environment patterns capture commonly used business integration topologies. A pattern provides you with a template for the deployment environment that you are creating.

      Note: Patterns have a direct relationship to the products supported by the configured deployment manager. WebSphere Process Server supports a specific set of patterns, with the *Remote messaging and remote support* pattern being the system default. If your deployment manager supports other products in addition to WebSphere Process Server, additional

patterns may apply. Consult product-specific documentation for information on patterns as they apply to the products.

For information on the types patterns included with and supported by WebSphere Process Server, see Topology types and deployment environment patterns in the Planning section.

See Custom deployment environment layout configuration for information on using the Custom Deployment Topology Detail page to configure your custom deployment environment.

b. Enter a unique name for the deployment environment in the **Deployment environment name** field.

c. **Optional:** To view all of the configuration steps in the wizard, select **Detailed: Show all steps**.

If you choose **Fast path: Show only needed steps** the wizard displays only those pages that **do not** have assigned default values. Choose **Fast path: Show only needed steps** only if you are agreeable to accepting the system-provided default values for the deployment environment configuration.

This topic assumes that you have chosen **Detailed: Show all steps**

d. Click **Next** to display the Deployment Environment Features page.

3. On the Deployment Environment Features page, select the feature for the deployment environment and click **Next** to either view a list of compatible features, or to view a list of deployment environment patterns. Features represent the runtime processing capabilities of your deployment environment.

The list of available features on the Deployment Environment Features page is based on the deployment manager profile. If your deployment manager profile has been augmented to include other products alongside WebSphere Process Server (for example, WebSphere Business Monitor or WebSphere Business Services Fabric), then the Deployment Environment Features page also lists these features.

If you have installed and configured a profile for WebSphere Process Server, then the Deployment Environment Features page includes the following:

- **WESB**, for WebSphere Enterprise Service Bus, which provides a deployment environment that supports mediations.
- **WPS**, for WebSphere Process Server, which provides a deployment environment that supports mediations, business processes, human tasks, and business rules.

The default value for the deployment environment feature matches the runtime capabilities of your deployment manager.

4. On the Select compatible deployment environment features page, select additional features as necessary and click **Next** to view the list of patterns associated with your primary and ancillary feature selections.

Note: The Select compatible deployment environment features page is displayed only if the deployment manager has been augmented with other business process management (BPM) features, such as WebSphere Business Monitor.

For an understanding of the relationship of features and compatible features, see the information on deployment environments in the Planning section.

5. On the Select the deployment environment pattern page, select the pattern for the selected deployment environment, then click **Next** to display the Select Nodes page.

The list of patterns that display on the Deployment Environment Patterns page is dynamic. This list is activated by, and dependent on, the following environment conditions and configuration decisions:

- The platform on which you have installed the software
- The selections that you have made on the Select the deployment environment feature page and the Select compatible deployment environment features page.

For a detailed description of the relationship of patterns to features, see Topology patterns and supported BPM product features

6. Optional: On the Select Nodes page, select the nodes that you want to include in this deployment environment, then click **Next** to display the Clusters page.

   Select at least one node for the deployment environment. For high-availability and failover environments, select at least two nodes. For scalability, select all nodes.

   To include a node, select the check box next to the node name. Use **Node Mapping** to map the selected node to another node name.

7. Optional: On the Clusters page, assign the required number of cluster members on each node for each cluster *type* (Application Deployment Target, Messaging Infrastructure and Supporting Infrastructure) of the deployment environment.

   By default one cluster member is assigned on each node for each function. You change the number by replacing the number in each column. If you are unfamiliar with the different cluster roles and functions provided by each type of cluster, see "Topology types and deployment environment patterns."

   A 0 (zero) value for a node means that the node does not contribute to the selected function, based on features that you have selected.

   After assigning cluster members, you can click **Next** to display the Cluster naming pages for each cluster type of the deployment environment. The Cluster naming sub-steps that display will vary depending on the deployment environment pattern selected.

   The system generates default values for cluster names and cluster member names.

   If you do not want to customize cluster names or cluster member names, you can use the wizard navigation pane to go directly to the REST Services page in a following step.

   Each substep page is structured in the same fashion, and is described in Customize the cluster names and cluster member names.

   a. Optional:

      Use the Cluster Naming page to customize cluster names or cluster member names for the cluster type. There is one substep page for each cluster *type* in the pattern that you have selected. For example, if you selected a **Remote messaging and remote support pattern**, there are 3 sub-steps, one for each type of cluster (Application Deployment Target, Messaging Infrastructure and Supporting Infrastructure) in that pattern.

      The information on each substep page is as follows:

      Cluster
      A read-only field specifying the functional role of the cluster.

      The value varies depending on the cluster type, as follows:
      - Application Deployment Target
      - Supporting Infrastructure

- Messaging Infrastructure

  For information on the functional role provided by each cluster type, see Topologies and deployment environment patterns

Cluster Name
Contains the system-generated default value for the cluster name.

Cluster Member Name
Accept the system-generated default value or specify a name of your choosing.

The default value for the cluster member name is based on the following naming convention: `<cluster name>.<node name>.<node number sequence>` .

The number of cluster member names that display in the table match the number of cluster members that you entered for the cluster type column and node row on the Clusters page. See the preceding step for the Clusters page.

8. On the REST Services page, configure service endpoints for Representational State Transfer (REST) application programming interfaces (APIs).

If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets.

   a. Configure a full URL path for all REST services by selecting either **https://** or **http://** from the **Protocol** list.

   b. Enter a name in the **Host Name or Virtual Host in a Load-Balanced Environment** field.

   c. In the **Port** field, enter the port that a client needs to communicate with the server or cluster.

   d. In the table of REST services, if you want to modify the description of the REST service endpoint, overtype the entry in the Description field. The other fields are read-only.

   e. Click **Next** to go to the Import the database configuration page.

9. Optional: On the Import the database configuration page, click **Browse** to go the database design document or enter the path to the database design document and then click **Next** to go to the Data sources page. The design document can be based on a database design that you created using the database design tool (DDT), or it can be the supplied design document based on the pattern and feature that you have selected.

   Note: The database design document that you import for the deployment environment does not change the commonDB created at Profile Creation time.

10. Conditional optional: Database page, configure the database parameters for data sources of the deployment environment, then click **Next** to go to the Security page.

On this page, define the database information for the components that are included in this deployment environment. Where possible, the wizard supplies default information for the parameters, but change those values to match the values that you defined when you planned the environment.

   Note: If you imported a database design document, the information on the Database page reflects the data source configuration as it exists in the database design document that you imported.

Whether or not this step displays for a fast path deployment environment configuration is conditional. This step displays for a fast path deployment environment configuration if more than one database has been defined.

This step always displays if you are using DB2 for z/OS or an Oracle database provider.

The default schema names that are displayed on this page might conflict with your site naming convention or might conflict with existing schemas. As such, it is likely that you will need to change the schema name.

Oracle database considerations:

- If you do not want to provide a DBA user name and password for all components when using Oracle, clear **Create tables** and specify preexisting and unique user names and passwords for each component. If you are able to provide a DBA user name and password for all the components, select **Create tables** and allow the configuration process to create the required schemas and users.

For a production environment, you should set the same values for **User name** and **Schema name** and you should deselect **Create tables**. For a production environment, create the required schemas manually and use the SQL files generated to create the tables.

Note: You cannot select **Create tables** for Business Space (the option is unavailable for selection). The SQL files for Business Space need to be run manually. For information on running the SQL manually for Business Space, see *Configuring Business Space database tables*.

You can edit all key parameters, such as the database name, whether or not to create tables, the data source runtime user name, and the password for the deployment environment.

You can select which database to use for the given component.

DB2 for z/OS: The **Create tables** option cannot be used if you are using a DB2 for z/OS database provider.

Steps that cannot be completed through the Deployment Environment Configuration wizard, and which need to be completed manually, are listed on the Deferred Configuration page.

11. On the Security page, configure the authentication aliases WebSphere uses when accessing secure components

    You can change the authentication alias user name and password on this page. These aliases are used to access secure components but do not provide access to data sources

12. On the Business Process Choreographer page, set parameters for the Business Process Choreographer configuration and then click **Next** to display the System web applications page. On this page you specify the values for:

    - Security roles
    - Authentication aliases

13. Optional: On the System web applications page, set the context root for component-based web applications in your deployment environment or accept the system-provided default values for the context roots. Then click **Next** to display the Summary page.

    The System web applications page displays for deployment environments using the Remote messaging, support and web applications pattern. The Remote messaging, support and web applications pattern applies if the deployment environment is for a deployment manager that has been augmented to include WebSphere Business Monitor.

The table contains the following control information.

Web Application
The name of the Web application.

Some of the components that are part of the deployment environment you are creating contain web applications. The **Web application** column can include the following components:
- Business Space
- Business Process Choreographer Explorer
- Business Rules Manager

Context Root
The current value of the context root for the component.

By default, the default context root for the web application applies. You can change the context roots by typing over the value in the **Context Root** field.

Note: The Business Space context root is read only and cannot be edited.

14. Verify that the information on the Summary page is correct and click **Finish and Generate Environment** to save and complete the configuration of the deployment environment. To exit without completing the configuration, click **Finish**.

Clicking **Finish** saves the deployment environment configuration - but does not generate it.

Click **Cancel** cancels the deployment configuration and does not save the configuration.

a. Check for deferred configuration steps

Select **Deployment Environments** → *name of deployment environment* → **Deferred Configuration**

You need to address any existing deferred configuration steps before starting the Deployment Environment.

Results

When the configuration completes, you can examine the configuration files to view the changes.

What to do next

Either save the changes to the master configuration or discard them.

Related concepts

➡ Deployment environments
A deployment environment is a collection of configured clusters, servers, and middleware that collaborates to provide an environment to host Service Component Architecture (SCA) interactions. For example, a deployment environment might include a host for message destinations, a processor of business events, and administrative programs.

➡ Topologies and deployment environment patterns
There are different topology layouts. Before you install and configureWebSphere Process Server, review the information in this section. Understanding topology concepts will help you to make educated decisions on how to install and configure the product.

"Configuring databases" on page 403
Includes information about database configuration for the Common database, Common Event Infrastructure, Business Process Choreographer, enterprise service bus logger mediation, messaging engine, selector and business rules group, and DB2 message logger database on a remote z/OS system.

Related tasks

➡ Configuring Business Space as part of the Deployment Environment Configuration wizard

➡ Configuring Business Space database tables

➡ General steps for implementing a deployment environment
After designing a deployment environment, you will perform specific tasks to make that design a reality. Regardless which method you use to implement the deployment environment, you will perform the same general steps.

"Configuring deferred configurations for a deployment environment" on page 471
If you must defer the creation of your databases and tables, use the Deferred Configuration page. This page provides instructions on how to locate and run scripts for database and table creation.

"Creating the database design file using the database design tool" on page 431
Use the database design tool (DDT) to generate a design file that is used to create the database tables required by WebSphere Process Server. The DDT generates the design file from a user specified properties file or user interactive input. The resulting design file is then used by the DDT to create the database scripts that are used to create the database tables. Additionally, the design file can be used as input during profile creation and during deployment environment configuration to specify the database configuration properties.

"Configuring custom deployment environments" on page 459
Use the Custom Deployment Topology Detail page to configure your custom deployment environment.

"Creating a deployment environment definition using the command line" on page 462
You can create a deployment environment definition using the wsadmin command. Running `createDeploymentEnvDef` provides the definition of the deployment environment.

Related information

➡ Configuring Business Process Choreographer

Custom deployment environment layout configuration:

This overview describes two major configuration considerations for custom deployment environments: selecting clusters and single servers to use with the environment and specifying the deployment environment configuration. An understanding of these considerations enables you to plan and implement a deployment environment effectively.

"Selecting Clusters and Single Servers to use with a deployment environment" on page 455 defines the clusters and servers that make up your deployment environment. Unlike the patterned deployment environments, where clusters are created for each function, in a custom deployment environment you add the clusters and servers that you need to perform functions.

"Defining the Deployment Environment Configuration" on page 455 describes the functions you configure for the clusters and servers. These functions are messaging, Common Event Infrastructure, or application support.

Before you complete the deployment environment configuration in the system by generating it, you can return to your configuration and make changes. After you generate the deployment environment configuration in the system, you can look at the current configuration. You can also add more servers and clusters, configure more functions, or you can remove servers and clusters from management by this deployment environment. You cannot undo a function configuration that you have already generated, and you cannot remove a server or cluster from the deployment environment definition that is still required by another server or cluster in your deployment environment.

Requirements for all custom deployment environments

A custom deployment environment layout includes these restrictions:
- After you complete a configuration by generating the deployment environment, the associated controls become checked and disabled. This means you cannot undo the configuration.
- After you generate the deployment environment, if a control is not checked and disabled for a component, you must configure the associated functions in the following order: configure the associated messaging engine, then configure the Common Event Infrastructure (CEI), then the application support (described later in this topic).
- The configurations that exist on a system override the topology layout configuration. Thus, exporting a custom topology reflects the actual configuration of the servers involved in the topology.

The Topology Layout page in the administrative console has four sections that you must configure for a custom topology:
- Select Cluster and Single Servers
- Messaging
- Common Event Infrastructure
- Components

The following sections include other requirements for completing a custom topology layout configuration.

Selecting Clusters and Single Servers to use with a deployment environment

Use the Select Cluster and Single Servers section of the Topology Layout page to manage the clusters and servers within the deployment environment and define which functions they provide.

The Select Cluster and Single Servers section of the Topology Layout page includes a list of available clusters and servers, which you configure as part of the deployment environment. You assign clusters and servers to collaborative units in the function configuration. Each collaborative unit represents a group of clusters and servers that provides, as a whole, a function in the deployment environment. You can remove clusters or servers from the deployment environment. However, you can remove only clusters or servers that are no longer needed by other clusters or servers in the configuration.

Defining the Deployment Environment Configuration

Use the Specify the Deployment Environment Configuration section of the Topology Layout page to define which clusters or servers participate in specific functions for the deployment environment.

Messaging

> **Note:** Partitioned messaging engines are not supported.

You use the fields in the Messaging tab to configure the messaging destination for selected targets. Each table represents one collaborative unit, and the Messaging section can include multiple tables. You must select only one target (Cluster/Server) for the option of local configuration for each unit, and all other targets in this unit assume the remote destination. When applications send messages to targets with a remote destination configuration, the system routes the messages to the local target for their unit.

The messaging configuration applies to the Service Component Architecture (SCA), the CEI, and the Business Process Choreographer system buses.

To prevent conflicts with the local destinations in your topology configuration, the following rules apply:

- The SCA system bus messaging engine configuration determines the local and remote destination locations. The SCA application, the CEI and the Business Process Choreographer bus configurations follow the SCA system bus configuration.
- If you locate the messaging engines for other buses on different targets in a unit, then the other targets in that unit assume the remote destination role. If the CEI or Business Process Choreographer buses have different configurations, an information message indicates that the messaging engine for a given bus is not located on the same target as the SCA messaging engine.
- If you try to add a target that already has a remote or local destination configured that conflicts with the current bus settings of a given unit, the system generates an error message.

Common Event Infrastructure
You configure CEI on the CEI tab. like Messaging. The CEI can have multiple tables, each representing a unit. In each table you select one CEI cluster or server (Cluster/Server column) that acts as the server by selecting the **Server** radio button. All targets that are not configured as a server assume the destination role. On the corresponding targets the event Infrastructure emitter

factory Java Naming and Directory Interface (JNDI) name is configured so that Common Base Events that are emitted on this target are sent to the server in their respective collaborative unit.

Application support

The Application Support tab lists all of the components that you can configure for a given deployment target. You configure component functions in a related collaborative unit. For example, you configure a Business Process Choreographer event collector in a unit to collect the Common Base Events that are emitted by the Business Process Choreographer container that is configured in the same unit. Each component configuration has requirements and dependencies on other component configurations. Dependencies are represented by cleared and disabled controls. To enable them, you must configure dependent controls first.

Note: Dependent controls are configured on either on the Messaging or the CEI tab.

Table 185 describes the relationships between the components.

Table 185. Deployment environment component relationships

Component	Purpose	Related Component	Considerations
Service Component Architecture (SCA)	Configures the deployment target for SCA application support. The SCA system and application bus members are configured locally if the corresponding messaging configuration is local; otherwise, they are configured remotely with the remote destination as specified in the corresponding messaging unit.	Messaging	SCA configuration is not available if you have not configured the deployment target for messaging.

Table 185. Deployment environment component relationships (continued)

Component	Purpose	Related Component	Considerations
Business Process Choreographer container	Configures the deployment target for both business flow and human task support. The configuration follows the SCA configuration for setting up the Business Process Choreographer system bus.	Messaging Service Component Architecture Business Process Choreographer Explorer	Business Process Choreographer configuration is not available if the deployment target has not been configured for messaging or if it has not been configured for Service Component Architecture support. One collaborative unit supports one Business Process Choreographer configuration. Add as many units as you need on the Application Support tab. To manage a container, consider configuring Business Process Choreographer Explorer.

Table 185. Deployment environment component relationships (continued)

Component	Purpose	Related Component	Considerations
Business Process Choreographer Explorer	Configures Business Process Choreographer Explorer on the selected deployment target. Business Process Choreographer Explorer is a Web application that manages the Business Process Choreographer container that is configured in the same collaborative unit. It includes an optional reporting function (Business Process Choreographer Explorer reporting) which was previously known as the *Business Process Choreographer Observer*.	Business Process Choreographer container	The Business Process Choreographer Explorer configuration is available after you have selected a Business Process Choreographer container configuration in the same collaborative unit. You must configure the deployment target for Web application support You can configure as many instances of Business Process Choreographer Explorer on a deployment target as you want. Add the deployment target to the collaborative units with a configured container and check the Business Process Choreographer Explorer configuration control.

Table 185. Deployment environment component relationships (continued)

Component	Purpose	Related Component	Considerations
Business Process Choreographer event collector	Configures the Business Process Choreographer event collector on the selected deployment target. The Business Process Choreographer event collector gathers Common Base Events that are emitted from the Business Process Choreographer container that is configured in the same collaborative unit. Statistical information about the observed container is recorded in a database.	Business Process Choreographer container Common Event Infrastructure	Configure first the Common Event Infrastructure server on the same deployment target that you plan to use for the Business Process Choreographer event collector. The Business Process Choreographer event collector is available only after you configure the Business Process Choreographer container in the same collaborative unit. If you are not sure whether you need to observe a given Business Process Choreographer container, you can configure this function later.
Business Rules Manager	Configures the Business Rules Manager on the selected deployment target. The Business Rules Manager allows you to configure business rules that determine business process behavior.	Service Component Architecture	The Business Rules Manager configuration control is available after you configure SCA support on the same deployment target. You can configure only one Business Rules Manager for a deployment environment. You might need to configure only one Business Rules Manager in your system because one instance can manage the business rules configuration of the entire cell.

Configuring custom deployment environments:

Use the Custom Deployment Topology Detail page to configure your custom deployment environment.

Before you begin

- Verify that deployment environments exist on this deployment manager.

Navigate to the administrative console of a deployment manager **Servers** → **Deployment Environments** → *deployment_environment_name* → **Additional Properties** → **Custom Deployment Topology Detail**.

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as an administrator or a configurator to perform this task.

Restrictions:

- The configurations that exist on a system take precedence over the deployment environment configuration. Thus, exporting a custom deployment environment reflects the actual configuration of the servers involved in the deployment environment.
- You need to configure the messaging units before configuring the component units. If the check box is unavailable, then you have not yet configured messaging support.

About this task

For a custom deployment environment, you can decide how to configure each function according to your needs. Configure each function to either clusters or single servers. There are three major areas in configuring a custom deployment environment topology:

- Messaging, which supports component internal communication.
- Common Event Infrastructure, which unifies event and monitoring functionality.
- Application Support, which supports business integration service components such as business processes and human tasks.

For more information see "Overview of custom deployment environment layout configuration."

Procedure

1. In **Select Clusters and Servers for use with this Deployment Environment**, select a cluster or server from the list.
2. Click **Add**. The cluster or single server will be added to the table below.
3. Repeat steps 1 and 2 until you have selected all the clusters and servers you need for this deployment environment.
4. Select the **Messaging** tab.
   a. Decide how many independent messaging units you need for your deployment environment and add that number by clicking **Add New Unit**.

      The system names each unit Messaging Unit *x*, where *x* is the number of the unit.
   b. Assign clusters and servers from the table created in step 2 to each unit.

      Select the cluster or server to add to the unit and then choose the unit from **Add selected to unit**.
   c. Decide which deployment target in each unit is to host local messaging support and configure the local messaging host by clicking **Local Bus Member** on the row that defines that deployment target in the unit.

All other clusters or servers are automatically configured for remote messaging destinations.

5. Click on the **Common Events Infrastructure** tab.

   a. Decide how many independent Common Events Infrastructure units you need for your deployment environment and add that number by clicking **Add New Unit**.

      The system names each unit Common Event Infrastructure Unit x, where x is the number of the unit.

   b. Assign clusters and servers from the table created in step 2 on page 460 to each unit.

      Select the cluster or server to add to the unit and then choose the unit from **Add selected to unit**.

   c. Decide which deployment target in each unit is to host the Common Event Infrastructure server and configure the Common Event Infrastructure server host by clicking **Server** on the row that defines that deployment target in the unit.

      All other clusters or servers are automatically configured for remote Common Event Infrastructure destinations.

6. Click on the **Application Support** tab. This tab shows all the components that can be configured for a given deployment target.

   Restriction: You must complete the messaging units for each component before you can configure the component in this section. For example, if the check box is unavailable for Service Component Architecture, then the associated messaging units have not been configured. See "Overview of custom deployment environment layout configuration" for additional restrictions.

   a. Decide how many independent Application Support units you need for your deployment environment and add that number by clicking **Add New Unit**.

      The number of units you need depends on how many Business Process Choreographer containers you need. If you do not need Business Process Choreographer containers a single unit will be sufficient for Service Component Architecture applications.

      The system names each unit Application Support Unit x, where x is the number of the unit.

   b. Assign clusters and servers from the table created in step 2 on page 460 to each unit.

      Select the cluster or server to add to the unit and then choose the unit from **Add selected to unit**.

   c. In a unit, select what cluster or server belongs to each component for your deployment environment.

   d. Repeat steps 6b and 6c until you configure all the components in each unit you need for your deployment environment.

What to do next

After completing or making edits to an existing deployment environment, the Custom Deployment Environment Configuration wizard opens. You can review the information and make any necessary changes.

Related concepts

➡ Deployment environments
A deployment environment is a collection of configured clusters, servers, and
middleware that collaborates to provide an environment to host Service
Component Architecture (SCA) interactions. For example, a deployment
environment might include a host for message destinations, a processor of business
events, and administrative programs.

➡ Topologies and deployment environment patterns
There are different topology layouts. Before you install and configureWebSphere
Process Server, review the information in this section. Understanding topology
concepts will help you to make educated decisions on how to install and configure
the product.

Creating deployment environments using the command line

You can use wsadmin to create a deployment environment. The
createDeploymentEnvDef and generateDeploymentEnv provide a command-line
equivalent to creating the deployment environment using the deployment
environment wizard.

Creating a deployment environment definition using the command line:

You can create a deployment environment definition using the wsadmin command.
Running createDeploymentEnvDef provides the definition of the deployment
environment.

Before you begin

You must be at the deployment manager from which you are creating deployment
environment definition.

Required security role for this task: When security and role-based authorization
are enabled, you must use a userid and password with administrator or operator
authority to perform this task.

WebSphere Process Server supports a specific set of patterns, **Remote messaging
and remote support** being the pattern to employ for a network deployment
production environment. If your deployment manager supports other products in
addition to WebSphere Process Server, the patterns for those products may apply.
Consult product-specific documentation for information on patterns as they apply
to the products. For more information on patterns see *Choosing your deployment
environment pattern* in the Planning documentation.

About this task

This task creates a deployment environment definition that is based on a specific
pattern and uses the wsadmincommand.

You can use the wsadmin command to create the same deployment environment
as you can create from the administrative console. This capability allows you to
run the administrative task to create a deployment environment definition with all
the default values based on an existing configuration. The existing configuration
being the configuration that you created at profile creation time. The command
also includes an optional property that imports a database design document. The
database design document holds the database configuration for the topology you

are creating. For more information database design documents, see *Creating the database design file using the database design tool* in Configuring databases.

A deployment environment definition describes the specific component, cluster/node/server configuration, resources and related configuration parameters that make up a deployment environment. This can also be referred to as an instance of a deployment environment configuration. A deployment environment configuration can be exported into a deployment environment definition. You can import a deployment environment definition to add a new deployment environment configuration to your system.

Procedure

1. Open a command window.

   The wsadmin command can be found at either the <WPS>/profiles/<dmgr profile>/bin directory, or the <WPS>/bin directory.

2. At the command prompt, enter the wsadmin command to enter the wsadmin environment.

3. Use the createDeploymentEnvDef command to create the deployment environment definition with a specific name for a particular runtime and pattern.

   Note: If administrative security is on, you will be prompted for a user ID and password, if you do not supply it in the command.

Example

This example creates a deployment environment definition for a remote messaging and remote support pattern on a WebSphere Process Server runtime, with myDepEnv on the host myDmgr with administrative security enabled. The example imports a database design document named **wps.nd.topology.dbDesign**:

```
wsadmin -connType SOAP -host myDmgr -port 8879
> $AdminTask createDeploymentEnvDef { -topologyName topOne
-topologyPattern RemoteMessagingAndSupport
-topologyRuntime WPS -dbDesign C:\dbDesigns\wps.nd.topology.dbDesign}
> $AdminConfig save
```

Note: If you disable administrative security, you do not need to provide a user ID and password.

Related tasks

"Creating a deployment environment using a pattern" on page 446
After you select a deployment pattern, use the Deployment Environment
Configuration wizard to create the deployment environment that is based on the
pattern.

Choosing your deployment environment pattern
You can configure your deployment environment by choosing one of the
IBM-supplied topology patterns or by creating your own custom deployment
environment. This topic section lists and describes the available IBM-supplied
topology patterns and presents considerations for choosing a topology.

"Creating the database design file using the database design tool" on page 431
Use the database design tool (DDT) to generate a design file that is used to create
the database tables required by WebSphere Process Server. The DDT generates the
design file from a user specified properties file or user interactive input. The
resulting design file is then used by the DDT to create the database scripts that are
used to create the database tables. Additionally, the design file can be used as
input during profile creation and during deployment environment configuration to
specify the database configuration properties.

Related reference

createDeploymentEnvDef command

Related information

Commands and scripts

Add nodes to a deployment environment definition using the command line:

You can add nodes to a deployment environment definition using the wsadmin
command.

Before you begin

The task assumes that the node has been federated to the deployment manager.

This command to add a node to the deployment environment definition will fail if
the topology is already configured.

You must be at the deployment manager to which you are adding nodes.

Required security role for this task: When security and role-based authorization
are enabled, you must use a userid and password with administrator or operator
authority to perform this task.

About this task

This task adds a federated node to a deployment environment definition and uses
the wsadmin command.

Procedure
1. Open a command window.
   The wsadmin command can be found at either the `<WPS>/profiles/<dmgr`
   `profile>/bin` directory, or the `<WPS>/bin` directory.
2. At the command prompt, enter the wsadmin command to enter the wsadmin
   environment.

3. Enter the addNodeToDeploymentEnvDef command to add the node to the deployment environment definition.

   Note: If administrative security is on, you will be prompted for a user ID and password, if you do not supply it in the command.

Example

This example adds a node (**MyNode**) to deployment environment definition (**myDepEnv**) with administrative security enabled:

Attention: If you are adding a node to a single cluster topology pattern, the value for -toplogyRole must be set to **ADT**. Deployment environment topology patterns are specified when you create the deployment environment using either the createDeploymentEnvDef command or the Deployment Environment Configuration wizard.

```
wsadmin -connType SOAP -host myDmgr -port 8879 -user dmgrAdmin -password dmgrPass
> $AdminTask addNodeToDeploymentEnvDef {-topologyName myDepEnv -nodeRuntime WPS
-topologyRole Messaging -nodeName MyNode -serverCount 3}
```

Note: If you disable administrative security, you do not need to provide a user ID and password.

Related reference

addNodetoDeploymentEnvDef command
Use the addNodeToDeploymentEnvDef command to add a node to an existing deployment environment definition.

Generating deployment environments using the command line:

You can generate deployment environments using the wsadmin interface. This capability allows you to configure multiple deployment environments unattended on a deployment manager using a script.

Before you begin

You must enter the commands on the deployment manager on which you are configuring deployment environments.

Required security role for this task: When security and role-based authorization are enabled, you must log in to the administrative console as an administrator or configurator to perform this task.

About this task

After you have imported or created deployment environments on a deployment manager, you can configure the deployment environments using the generateDeploymentEnv command.

Procedure

1. Enter the wsadmin environment.
2. Enter the generateDeploymentEnv command for each topology you are configuring.

Example

The following command configures the eastEnvironment and westEnvironment topologies on host myDmgr.

```
wsadmin -connType SOAP -host myDmgr -port 8879
> $AdminTask generateDeploymentEnv -topologyName eastTopology
> $AdminTask generateDeploymentEnv -topologyName westTopology
> $AdminConfig save
```

Note: If administrative security is enabled, you are prompted for a user ID and password after the system processes the wsadmin command.

What to do next

Save the configured deployment environments. From the command line, enter `$AdminConfig save`.

Related information

generateDeploymentEnvFromDef command

Importing deployment environment definitions using the command line

Managing node agents

Validate the deployment environment definition from the command line:

You can validate the deployment environment definition using the wsadmin command.

Before you begin

The task assumes that the node has been federated to the deployment manager.

You must be at the deployment manager to which you are validating the deployment environment definition.

Required security role for this task: When security and role-based authorization are enabled, you must use a userid and password with administrator or operator authority to perform this task.

About this task

This task validates the deployment environment definition and uses the wsadmin command.

Procedure

1. Open a command window.

   The wsadmin command can be found at either the `<WPS>/profiles/<dmgr profile>/bin` directory, or the `<WPS>/bin` directory.

2. At the command prompt, enter the wsadmin command to enter the wsadmin environment.

3. Enter the validateDeploymentEnvDef command to validate the deployment environment definition.

   Note: If administrative security is on, you will be prompted for a user ID and password, if you do not supply it in the command.

Example

This example validates the deployment environment definition (**myDepEnv**) with
administrative security enabled:

```
wsadmin -connType SOAP -host myDmgr -port 8879 -user dmgrAdmin -password -dmgrPass
> $AdminTask validateDeploymentEnvDef { -topologyName topOne}
```

Note: If you disable administrative security, you do not need to provide a user ID
and password.

Related reference

validateDeploymentEnvDef command

Related information

Commands and scripts

Displaying deployment environment status using the command line:

You can display the current status of a deployment environment using the
wsadmin command.

Before you begin

The admin client must connect to the deployment manager for which you are
displaying the status.

Required security role for this task: When security and role-based authorization
are enabled, you must use a userid and password with administrator or operator
authority to perform this task.

About this task

This task displays the current status of a deployment environment and uses the
wsadmin command.

Procedure

1. Open a command window. .

   The wsadmin command can be found at either the `<WPS>/profiles/<dmgr
   profile>/bin` directory, or the `<WPS>/bin` directory

2. At the command prompt, enter the wsadmin command to enter the command
   environment.

   Note: Make sure wsadmin connects to the correct deployment manager, when
   running in connected mode.

3. Use the showDeploymentEnvStatus command to show the current status of the
   deployment environment.

   Note: If administrative security is on, you will be prompted for a user ID and
   password, if you do not supply it in the command.
   The following table lists the results that might be returned.

   Note: Some of the states listed in the table are valid for configured topologies
   only. The states that are apply to configured topologies only are noted as such.

Table 186. States of a topology instance in order of least to most available

State	Description
Incomplete	The deployment environment is not missing any elements but is incomplete in some way. Incomplete state may mean the deployment environment is missing a required role, node, comp or dependencies . The warning message contains additional details.
Complete	This state is also known as *Not configured* and it means that the configuration is known and complete but has not yet been generated.
Configured	This means the configuration is in synch.
Partially configured	The deployment environment has been generated but deferred configuration has not been completed.
Unknown	The system cannot determine the current state of the deployment environment. A resync operation could be performed on this state.
Stopped	State applies to configured topologies only.All deployment targets in the topology are stopped.
Running	State applies to configured topologies only.The deployment environment is available and all functions are running.
Partially started	State applies to configured topologies only.The deployment environment is available but at least one function is partially running.
Starting	State applies to configured topologies only.The deployment environment is starting.
Partially stopped	State applies to configured topologies only.The deployment environment is available but at least one function is stopped or partially stopped.
Stopping	State applies to configured topologies only.The deployment environment is stopping
Unavailable	State applies to configured topologies only.The deployment environment state is unavailable.

Example

This example displays the status of a deployment environment (**MyDepEnv**) on the host (**myDmgr**) with administrative security enabled.

Note: If you are running the admin client from the deployment manager bin folder, you do not need to include the -host and -port parameters in the command.

```
wsadmin -connType SOAP -host myDmgr -port 8879 -user dmgradmin -password dmgrpass
> $AdminTask showDeploymentEnvStatus {-topologyName myDepEnv}
```

The -connType parameter specifies the type of connection to be used; the default argument is SOAP.

Note: As the default is SOAP, you do not need to give explicitly if SOAP is the connection type that is being used.

The -host parameter specifies the host used for the SOAP or RMI connection. The default value for -host is the local host.

Note: If the node is running on the local host, you don not need to specify -host

Note: If you disable administrative security, you do not need to provide a user ID and password.

Related information

Commands and scripts

showDeploymentEnvStatus command

Editing deployment environment settings

You can edit and modify the deployment environment settings

Configuring host aliases

Configure the IBM HTTP server or a server of your choice to allow communication between managed nodes and the deployment manager.

Before you begin

Create and configure a deployment manager and associated nodes.

About this task

The managed nodes and the deployment manager must be able to communicate with each other, so the host name alias for each node in the deployment target cluster must be visible to the deployment manager. The host name alias consists of the DNS host name and port number. You use this alias as part of a URL to access applications when they are running on the deployment target.

Note: This procedure uses two application cluster members that are referred to as AppCluster_member1 and AppCluster_member2. Substitute your server names in the instructions.

Procedure

1. From the administrative console, navigate to **Servers** ➤ **Server Types** ➤ **WebSphere application servers** ➤ *AppCluster_member1*.
2. Click the name.
3. Under the Communications heading, expand **Ports** and note the port value listed for *WC_defaulthost*. You will need to use it later.
4. Repeat steps 1 through 3, for every cluster member. Repeat this for each additional application cluster member.

   When you are finished, you will have a list of the cluster members and the port numbers for their default host.
5. From the administrative console, navigate to **Environment** ➤ **Virtual Hosts** ➤ **default_host**.
6. Under **Additional Properties**, click **Host Aliases**.
7. If an entry for the correct combination of host name and port value for cluster members is not displayed, add the missing entries to the list.
8. If you added new entries to the list, click **Save** and then **Synchronize**.

What to do next

Verify your installation by installing a test application.

Configuring a data source for your deployment environment

Configure your business integration data source for the first time using the Database Provider Configuration page.

Before you begin

- Verify that deployment environments exist on this deployment manager.
- Navigate to the administrative console of a deployment manager **Servers** → **Deployment Environments** → *deployment_environment_name* → **Related Items** → **Data Sources**.

Required security role for this task: When security and role-based authorization are enabled, you must log in to the administrative console as an administrator or configurator to perform this task.

About this task

Use the Data Sources page to configure the collection of all the data sources that are needed in your deployment environment.

The component that needs the data source determines all required fields based on the **Database Provider** selected, and these fields must be completed. The component completes the rest of the fields with default values. You may either keep the default values or change them to meet your needs. In most cases, the component determines the **Scope** value.

You can configure a business integration data source only once. After you configure the data source and save it, some text boxes will be unavailable and you cannot change the values. All other text boxes on the page can be edited.

Procedure

1. In the Data Sources page, select check box next to the data source to configure.
2. Click **Edit Provider** to edit additional data source fields that are not shown on this page.

   Note: Alternatively, you can just click the name of the data source in the **Data Source** column.
3. Enter the information. For a list of supported database types, see "Database specifications."
4. Click **Apply** or **OK** to save your changes.

Related information

Configuring databases
Includes information about database configuration for the Common database, Common Event Infrastructure, Business Process Choreographer, enterprise service bus logger mediation, messaging engine, selector and business rules group, and DB2 message logger database on a remote z/OS system.

Common database specifications
The Common database configurations contain information about supported database types; scripts and their locations; profile creation configuration actions; installation parameters; types of created tables and user ID privileges.

Configuring authentication aliases for a deployment environment
From one administrative console page, you can review or edit all your authentication aliases.

Before you begin

- Verify that deployment environments exist on this deployment manager.

Navigate to the administrative console of a deployment manager **Servers** →
Deployment Environments → *deployment_environment_name* → **Related Items** →
Authentication Aliases.

Required security role for this task: When security and role-based authorization
are enabled, you must log in to the administrative console as an administrator or
configurator to perform this task.

About this task

From this consolidated list of authentication aliases, you can:
• Review all the aliases for a given deployment environment
• Access the authentication configuration page through the *Alias_name* link

The **Reset** button resets the selected rows to the currently configured values. Click
Alias_name to access the authentication configuration page where you make your
changes.

Procedure
1. Select the row you want to change.
2. Do one of the following:

Option	Description
To edit the row	Click *Alias_name*.
To reset the row	Click **Reset**.

   Editing a row takes you to the authentication configuration page where you
   make your changes.
3. Click **OK** or **Apply** to save any changes.

Related information

Authentication

Configuring deferred configurations for a deployment environment
If you must defer the creation of your databases and tables, use the Deferred
Configuration page. This page provides instructions on how to locate and run
scripts for database and table creation.

Before you begin
• Verify that deployment environments exist on this deployment manager.

Navigate to the administrative console of a deployment manager **Servers** →
Deployment Environments → *deployment_environment_name* → **Additional
Properties** → **Deferred Configuration**.

Required security role for this task: When security and role-based authorization
are enabled, you must log in to the administrative console as an administrator or
configurator to perform this task.

About this task

Use this procedure when you must create database tables or schemas separately
from configuring a deployment environment.

The Deferred Configuration page shows the configuration steps needed to correctly configure your topology's databases. In most cases this page shows:

- Script location
- Instructions on how to run the scripts

Procedure

1. Perform the instructions provided in the Deferred Configuration page.
2. When you finish, click **Configuration Done**.

What to do next

A text box shows by whom and when the deferred configuration was performed last. The displayed instructions remain on this page for future reference.

Related tasks

"Creating a deployment environment using a pattern" on page 446
After you select a deployment pattern, use the Deployment Environment Configuration wizard to create the deployment environment that is based on the pattern.

Verifying your deployment environment

Before moving your production applications to the new environment, you must test to make sure that all of the components operate correctly.

Before you begin

Complete the implementation of your deployment environment as described in "Implementing a deployment environment."

1. Install the software
2. Configure a node to host a deployment manager
3. Configure nodes
4. Federate nodes to the deployment manager
5. Cluster nodes together to provide function for the deployment environment

About this task

How you verify the deployment environment depends on whether the environment you implemented is an IBM-supplied deployment environment or a custom deployment environment. You can manage IBM-supplied deployment environments from a single panel in the administrative console. You must create and manage custom deployment environments manually in the administrative console.

Procedure

1. Identify the type of deployment environment you are verifying.
   You should already have this information based on your original plans.
2. Start the deployment environment.

Type of deployment environment	How to start
IBM-Supplied pattern	Start from **System administration > Deployment environments > Deployment environment configuration** as described in "Starting and stopping deployment environments."
Custom	Start from **Servers > Clusters** as described in "Verifying a custom deployment environment starts." **Note:** You must start all the servers and clusters defined in the deployment environment.

3. Install the test application.
4. Configure the test application for routing.
5. Start the test application.
6. Run the test application and verify those results.

What to do next

Install your production applications.

Verifying the application deployment target cluster starts

To verify that the application deployment target cluster can start, you must start all the clusters in your deployment environment. This is an example for a three cluster deployment environment.

Before you begin

You need to create and configure the clusters for the messaging engines, Common Event Infrastructure (CEI) event server application and the application deployment target.

About this task

To verify that the application deployment cluster can start, you will start each cluster in turn.

Notes:

- This description assumes that you configured three clusters in the topology named MECluster, SupportCluster, and AppCluster. Substitute the actual cluster names and repeat the appropriate steps for any additional clusters in your deployment environment.
- The first time you start servers will take longer than subsequent starts because the system is creating the database tables and schemas.

Procedure

1. From the administrative console on the deployment manager, expand **Servers**, then select **Clusters**.
2. Start the clusters.
   a. Select the check box beside **MECluster**.
   b. Select **Start**, and wait for the MECluster to start as shown by a green arrow.
   c. Select the check box beside **SupportCluster**.

    d. Select **Start**, and wait for the SupportCluster to start as shown by another green arrow.

    e. Select the check box beside **AppCluster**.

    f. Select **Start**, and wait for the AppCluster to start as shown by another green arrow.

3. Click the messaging buses.

    a. Wait until all the clusters start.

    b. Click **Service Integration** → **Buses**

    c. Verify the messaging engine is running for each bus.

        1) Select the bus name.

        2) Click **Local Topology** to display the bus topology.

        3) Expand the bus until you see the status of the messaging engines.

4. Check the cluster members' SystemOut.log and SystemErr.log files located in the profile directory's logs subdirectory on the node that hosts the cluster member. Make sure that they have no errors, and look for the line `Server AppCluster_member1 is open for e-business` or `Server AppCluster_member2 is open for e-business` indicating that the cluster started successfully. Correct any errors you find before continuing.

What to do next

After correcting any errors, you configure the host aliases.

Note: After correcting configuration errors, you must stop the cluster and restart it for the configuration changes to take effect.

Troubleshooting tip: When examining the log you may see a message that states that a messaging engine failed to start because it could not find a certain bus. Restarting the clusters eliminates this message.

Installing the test application

Install the test application to begin the process of verifying your deployment environment.

Before you begin

- You need to create and install your completed deployment environment.
- Log in to the deployment manager administrative console.

About this task

Use the application provided for you with WebSphere Process Server called BPCIVTApp (Business Process Choreographer Installation Verification Test) to verify that you installed and configured your WebSphere Process Server environment correctly. First you must install the application.

For more information about installing this application, see "Verifying that Business Process Choreographer works". For more information about installing applications from the administrative console, see "Installing application files with the console."

Note: If you have not enabled business processes and human tasks, you cannot use BPCIVTApp to test your deployment environment. In this case, you must install and run a Service Component Architecture application that uses business

rules and selectors to exercise your deployment environment. Change the process to test the deployment environment to fit your application.

Procedure

1. From the administrative console, select **Applications** ‣ **New Application** ‣ **New Enterprise Application**.
2. Make sure that **Local file system** is selected, and then browse for the file `bpcivt.ear`. It will be in the *install_root*/installableApps directory.
3. Select the file `bpcivt.ear`, then select **Open**.
4. These steps assume you will use the default configurations. Select **Next** on the subsequent panels until you reach the Summary page. During these steps you will be selecting various options and mapping the module to the servers as described in other topics. For testing purposes, map this module to the application deployment target cluster.

   Note: You will not have to map the module to the application target cluster on a stand-alone server.
5. Select **Finish**.
6. Select **Save**, then **Synchronize**.

What to do next

Configuring the test application for routing:

Use this procedure to configure your test application for routing.

Before you begin

You need to install your test application.

About this task

You first configure the application and then generate the plug-in configuration files.

Note: The description assumes a cluster named AppCluster and a Web server named Webserver1. If your test application uses human tasks or business processes, make sure you have already configured Business Process Choreographer on your application cluster.

For information on managing modules, module settings and mapping modules, see the WebSphere Application Server information center.

Procedure

1. Configure the application (or applications) that you will run to identify the Web server and the deployment target to the application, as follows.
   a. From the administrative console, select **Applications** ‣ **Application Types** ‣ **WebSphere enterprise applications**.
   b. Select the name of the application.
   c. Select **Manage modules**.

   On this panel, each Module must map to one or more targets, identified under Server.

d. From the choices listed under Clusters and servers, select *Webserver1* (the Web server you configured previously) and *AppCluster* (the application deployment target).
   e. Select **Apply**, then select **OK**.
   f. Repeat steps 1d through 1e until you have configured all Web servers and deployment targets for your deployment environment.
   g. Select **Save**, then **Synchronize**.
2. Generate the plug-in configuration file.
   a. From the administrative console, select **Servers** → **Server Types** → **Web servers**.
   b. Select the check box next to the name *Webserver1*.
   c. Select **Generate plug-in**. A plug-in configuration file is created, as indicated by the message in the top of the window.
   d. Repeat steps 2b and 2c as many times as needed for your deployment environment.

What to do next

Stop and restart the deployment manager and node agent. Next start the test application.

Starting the test application:

Use this procedure to start your test application to test your implementation.

Before you begin

You need to install and configure the test application for routing.

About this task

You start your test application from the administrative console.

Procedure

1. From the administrative console, select **Applications** → **Application Types** → **WebSphere enterprise applications**.
2. Select the check box next to the application name and select **Start**. Wait until a green arrow appears, indicating that the application has started successfully.

What to do next

After you start the test application, run this application.

Note: If the application does not start correctly, refer to the log files to find error messages indicating the problem.

Running the test application:

Use this procedure to run your test application to determine if your deployment environment is operating correctly.

Before you begin

You need to start your test application.

About this task

Successful execution of this application shows that your deployment environment is operating correctly. Follow the same procedure on the other member of the application deployment target cluster to make sure that it also functions correctly.

Procedure
1. In a browser window, enter a URL in the following form: `http://hostname:portnumber/testapp` where *hostname* is the fully qualified DNS name or IP address of the system hosting the cluster member on which you installed the application, and *portnumber* is the port number associated with default host for that cluster member and *testapp* is the name of your test application.
2. Examine the logging messages on the screen.

   If your test application contains human tasks, you should see logging messages being written to the screen starting with `Looking up the HumanTaskManager API EJB...`. The application will proceed to create a task, claim it, check input and output data, complete the task, and delete it. The word `Passed` appears near the end of the log messages to indicate that the application ran successfully.

   Make sure that you see all messages you have embedded in your application to indicate success.

What to do next

Install and start other test applications.

Installing and accessing other applications

Install and access applications from the administrative console or Business Process Choreographer Explorer to further test your deployment environment.

Before you begin

You must have successfully installed and configured a deployment environment.

About this task

You can install and start other applications similarly to the way you installed your test application. To access these applications you will use the administrative console or Business Process Choreographer Explorer.

Procedure
1. Locate your application.

   In the administrative console click **Applications** → **New Application** and locate the application to install.
2. Install the application.
3. Start the application.
4. Access the application.

   Enter a URL for the application in a browser window. For example, `http://hostname:portnumber/myapp` where *hostname* is the fully qualified DNS name (or IP address) of the system corresponding to the cluster member on which you've installed the application, *portnumber* is the port number associated with default_host for that cluster member, and *myapp* is the name of the application that you want to access.

   From Business Process Choreographer Explorer:

a. Enter a URL in the following form in a browser window: `http://hostname:portnumber/bpc` where *hostname* is the fully qualified DNS name (or IP address) of the system corresponding to the cluster member, on which you've installed the application, and *portnumber* is the port number associated with default_host for that cluster member.

A page will appear labeled **My Tasks**, but with no tasks listed.

b. Select **My Process Templates**. You should see templates listed corresponding to any applications that you installed.

c. Use the interface controls on the page to start a task, work on it, complete it, and so on. For more information on running Business Process Choreographer tasks, see "Administering business processes and human tasks."

5. If desired, you can check the `SystemOut.log` file for the cluster member to view a record of the application and check for errors.

Configuring SCA support for a server or cluster

Use the Service Component Architecture (SCA) console page to enable a server or cluster in a network deployment environment to host service applications, their required messaging engines and destinations, or both.

Before you begin

Before configuring SCA support, determine the following:

- Whether you are using a stand-alone server profile. If so, SCA support is already configured and you cannot use the Service Component Architecture page to remove that support; however, you can use this page to modify some properties for database data sources.
- Where to host the messaging engines and destinations (use either a local or remote bus member).
- Whether you need to configure the SCA system bus only, or whether you also need to configure the SCA application bus. The application bus is configured by default and is required if you plan to deploy SCA applications that use WebSphere Business Integration Adapters.

Security role required for this task: You must be logged in as administrator or configurator to perform the following task.

About this task

Service applications require the use of one or more of the automatically created service integration buses, which must have configured messaging engines for destinations. By default, new servers and clusters in a network deployment configuration are not configured to host SCA applications and their destinations.

To configure SCA support on your server or cluster, perform the following steps.

Procedure

1. From within the administrative console, click one of the following, depending on your scope:
   - **Servers** → **Server Types** → **WebSphere application servers** → *server_name* → **Service Component Architecture**

- **Servers → Clusters → WebSphere application server clusters → *cluster_name* → Service Component Architecture**

2. Click **Support the Service Component Architecture components**.

3. In the Bus Member Location panel, specify where you want to host the destinations and messaging engines required by the SCA applications. There are two options:

   - **Local**. Specifies that you plan to host SCA applications, destinations, and messaging engines on the current server or cluster.

   - **Remote**. Specifies that you plan to host SCA applications on the current server or cluster while hosting destinations and messaging engines on a remote server or cluster (also referred to as a *deployment target*).

4. **(Remote bus member only)** If you selected **Remote** in the previous step, specify the remote server or cluster you want to use to host application destinations and messaging engines. Use the drop-down menu to select an existing deployment target (one that is already configured as a member of the SCA system bus), or click **New** to select a new server or cluster from the Browse Deployment Target page.

   If you select a new server or cluster from the Browse Deployment Target page, the necessary messaging is automatically configured on that target when you complete the SCA configuration documented in this topic.

5. Use the table in the System Bus Member panel to verify or modify the system bus data source configuration.

   a. Verify any default values in the **Database name**, **Schema**, **Create Tables**, **User name Password**, **Server**, and **Provider** fields. See the online help for detailed information about these fields and the values they accept.

   b. If no default values exist in these fields, or if the default values are incorrect, enter the appropriate values for the system bus data source. You can enter values directly in the field or by clicking **Edit** and making edits on the Data Source details page.

   c. Optional: Ensure that the data source can contact and authenticate with the database by clicking **Test Connection**.

6. Use the table in the Application Bus Member panel to verify or modify the application bus data source configuration.

   a. Ensure the **Enable the WebSphere Business Integration Adapter components** option is selected.

      Note: If you do not want to use the application bus, clear the **Enable the WebSphere Business Integration Adapter components** option and proceed to Step 7.

   b. Verify any default values in the **Database name**, **Schema**, **Create Tables**, **User name Password**, **Server**, and **Provider** fields. See the online help for detailed information about these fields and the values they accept.

   c. If no default values exist in these fields, or if the default values are incorrect, enter the appropriate values for the application bus data source. You can enter values directly in the field or by clicking **Edit** and making edits on the Data Source details page.

7. Click **OK** to complete the SCA configuration.

8. Save your changes. You can also optionally review the changes you have made.

Considerations for Service Component Architecture support in servers and clusters

Servers and clusters can support Service Component Architecture (SCA) applications, application destinations, or both.

SCA applications (also called service applications) require the use of one or more of the automatically created service integration buses. Each application uses a set of messaging resources, which are called *destinations*. These destinations require configured messaging engines, and they can be hosted on the same server or cluster as the application or on a remote server or cluster. Messaging engines typically use database data sources; note that a file store can be used in place of a database data source in a stand-alone server profile if that option was selected during profile creation.

By default, new servers and clusters in a network deployment or managed node environment are not configured to host SCA applications and their destinations.

Note: A stand-alone server has SCA support automatically configured. You cannot disable this configuration.
To enable this support, use the Service Component Architecture page in the administrative console. For servers, ensure that the application class-loader policy is set to `Multiple`.

Before enabling SCA support for a server or cluster in a network deployment or managed node environment, determine which of the following possible configurations you want to implement:

- **Remote bus member configuration**: The server or cluster hosts SCA applications, but the destinations are hosted on a remote server or cluster. This scenario requires the remote service integration bus members to be configured with the messaging engines needed to host the destination.

  While the use of remote messaging requires initial investment in planning for and configuring the service integration bus and its members, that configuration can be reused by multiple members within the application cluster. Messages are distributed to every member. In addition, the initial configuration can be structured to provide failover support.

- **Local bus member configuration**: The server or cluster hosts both SCA applications and application destinations. The required messaging engines are configured using the local bus members on the server or cluster.

Refer to the planning topics to help you decide which configuration is appropriate for your environment.

Related information

⇨ Configuring class loaders of a server

⇨ Learning about service integration buses

⇨ Messaging engines

Configuring all REST services on the administrative console

Configure all Representational State Transfer (REST) services for your environment by using the REST service administrative console page.

Before you begin

Before you complete this task, you must have installed your WebSphere business process management product.

About this task

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the administrative console page allows you to configure REST services for all of your product's widgets in Business Space. On the REST Services page, you can view all services for your environment and enable or disable each service individually.

Procedure

1. Click **Services** ⇒ **REST services** ⇒ **REST services**.

   The REST Services page opens, displaying all REST services in your environment.

2. For the **Scope section**, designate all to view all REST services in your environment, or select a server or cluster where you have REST services enabled.

3. In the table that lists the REST services for the provider, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.

4. For each individual service that you want to enable, type a meaningful description in the **Description** column.

5. Click **OK** to commit the changes to the services.

Configuring REST services in a service provider

Configure Representational State Transfer (REST) services in a service provider by using the REST service providers configuration administrative console page.

Before you begin

Before you complete this task, you must have installed your WebSphere business process management product.

About this task

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the administrative console page allows you to configure REST services. On the REST service providers configuration page, you can view all services for a selected service provider and enable or disable each service individually. If you prefer to manage REST services by your server or cluster (or by business processes or human task components), use the REST Services administrative console page.

Procedure

1. Click **Services** ⇒ **REST services** ⇒ **REST service providers** ⇒ .

   The REST service providers page opens, displaying all REST service providers.

2. Click a provider link to configure the services for the group of REST services managed by that provider.

   The REST service providers configuration page opens, displaying all REST services in the provider.

3. Select a **Protocol** from the list for all REST services that you want to configure so they are available in your runtime environment. Configure a full URL path by selecting either **https://** or **http://** and then type the **Host Name or Virtual Host in a Load-Balanced Environment** and **Port**. Use a fully qualified host name.

   If you want REST requests to go directly to the application server, type the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, type the host name and port of the proxy server or HTTP server that you have already set up. In an environment with a load balancer or proxy server between the browser and the Business Space and REST services, make sure that what you designate for the protocol, host, and port matches the browser URL for accessing Business Space.

4. In the table that lists the REST services for the provider, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.

5. For each individual service that you want to enable, type a meaningful description in the **Description** column.

6. Click **OK** to commit the changes to the services.

Configuring REST services for a server, cluster, or component

Configure Representational State Transfer (REST) services for a server, cluster or a component by using the REST Services administrative console page.

Before you begin

Before you complete this task, you must have installed your WebSphere business process management product.

About this task

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the REST Services administrative console page allows you to configure services for a server, a cluster, or a component.

Procedure

1. Click one of the following.
   - For system REST services on a server, click: **Servers** → **Server Types** → **WebSphere application servers** → *name_of_server* → **Business Integration** → **REST Services**
   - For system REST services on a cluster, click: **Servers** → **Clusters** → **WebSphere application server clusters** → *name_of_cluster* → **Business Integration** → **REST Services**
   - For business process REST services on a server, click: **Servers** → **Server Types** → **WebSphere application servers** → *name_of_server* → **Business Integration** → **Business Flow Manager** → **REST Services**
   - For business process REST services on a cluster, click: **Servers** → **Clusters** → **WebSphere application server clusters** → *name_of_cluster* → **Business Integration** → **Business Flow Manager** → **REST Services**
   - For human task REST services on a server, click: **Servers** → **Server Types** → **WebSphere application servers** → *name_of_server* → **Business Integration** → **Human Task Manager** → **REST Services**

- For human task REST services on a cluster, click: **Servers** → **Clusters** → **WebSphere application server clusters** → *name_of_cluster* → **Business Integration** → **Human Task Manager** → **REST Services**

  The REST Services page appears, displaying all default REST services that you can configure for use with your server or cluster (or Business Flow Manager or Human Task Manager component). If a REST service has already been configured, you see a message displayed.

2. Select a **Protocol** from the list for all REST services that you want to configure so they are available in your runtime environment. Configure a full URL path by selecting either **https://** or **http://** and then type the **Host Name or Virtual Host in a Load-Balanced Environment** and **Port**. Use a fully qualified host name.

   If you want REST requests to go directly to the application server, type the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, type the host name and port of the proxy server or HTTP server that you have already set up. In an environment with a load balancer or proxy server between the browser and the Business Space and REST services, make sure that what you designate for the protocol, host, and port matches the browser URL for accessing Business Space.

3. In the table of REST services, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.

4. In the table of REST services, type a meaningful description for each of the REST services in the **Description** field.

5. Click **OK** to commit the changes to the services.

   To modify the REST service configuration at later time, you can come back to the REST Services page or you can use other administrative console pages to manage the configuration of REST service endpoints. The REST service providers page allows you to select service provider that you want to configure. The REST services page accessed from **Services** → **REST services** allows you to configure all REST services in your environment.

Configuring REST services using the command line

Representational State Transfer (REST) services must be configured before you can use them in your runtime environment. If you do not use the REST Services administrative console page, use the updateRESTGatewayService command.

Before you begin

Before you complete this task, you must have installed your WebSphere business process management product.

For WebSphere Process Server, if you have configured Business Process Choreographer, the Human Task Management REST services are already configured. However the REST Services Gateway application, which is a service provider for other REST services, must be configured with the updateRESTGatewayService command.

Procedure

1. Open a command window.

The wsadmin command can be found in the *profile_root*/bin directory for a stand-alone server environment, or in the *deployment_manager_profile_root*/bin directory for a network deployment environment.

2. At the command prompt, type the wsadmin command to start the wsadmin environment.

3. Use the updateRESTGatewayService command to configure REST services specifying the cluster or the server and node. The **-enable** parameter is optional, and if not specified, defaults to true.

4. Run save command.

Example

The following example uses Jython to run the updateRESTGatewayService command and then save the changes. It configures the REST services on a cluster.

```
AdminTask.updateRESTGatewayService('[-clusterName
 cluster_name]')
AdminConfig.save()
```

The following example uses Jacl:

```
$AdminTask updateRESTGatewayService {-clusterName
 cluster_name}
$AdminConfig save
```

Configuring Business Process Choreographer

For information on how to configure Business Process Choreographer, go to the WebSphere Process Server for Multiplatforms, version 7.0, information center and review the topics under **Configuring WebSphere Process Server > Configuring Business Process Choreographer**. You can also find this information in the *Business Process Choreographer* PDF.

Configuring Business Space

Install and configure Business Space powered by WebSphere to set up a common interface for application users to create, manage, and integrate Web interfaces across the IBM WebSphere business process management portfolio.

Before you begin

You must install the product software. When you install your product, Business Space files are included with the installation for the profiles that you configured.

For WebSphere Process Server runtime environments that need the Human Task Management widgets, you must configure Business Process Choreographer. For more information, see Configuring Business Process Choreographer in the WebSphere Process Server documentation.

About this task

Business Space is supported with the following database products to match support for the WebSphere product you are using:

- Derby Embedded (for WebSphere Business Monitor, WebSphere Business Services Fabric, WebSphere Enterprise Service Bus, and WebSphere Process Server).

- Derby Network Server (for WebSphere Business Monitor, WebSphere Enterprise Service Bus, and WebSphere Process Server).
- DB2 Universal (for WebSphere Business Compass, WebSphere Business Monitor, WebSphere Business Services Fabric, WebSphere Enterprise Service Bus, and WebSphere Process Server).
- DB2 for IBM i (for WebSphere Enterprise Service Bus and WebSphere Process Server).
- DB2 for z/OS (for WebSphere Business Monitor, WebSphere Business Services Fabric, WebSphere Enterprise Service Bus, and WebSphere Process Server).
- Microsoft SQL Server Enterprise 2005 SP 2 and 2008 (for WebSphere Business Services Fabric, WebSphere Enterprise Service Bus, and WebSphere Process Server).
- Oracle 11g (for WebSphere Business Compass, WebSphere Business Monitor, WebSphere Business Services Fabric, WebSphere Enterprise Service Bus, and WebSphere Process Server).

Monitor **Process Server / ESB** If you install WebSphere Process Server, WebSphere Enterprise Service Bus, or WebSphere Business Monitor and create a stand-alone server profile with the typical option, Business Space is installed and configured automatically with a Derby Embedded database. If you are using a stand-alone server profile, you can use the Profile Management Tool with the advanced option to configure Business Space to work with your runtime environment. For more information, see "Configuring Business Space using the Profile Management Tool."

For all products, if you are setting up deployment manager and custom profiles, the simplest way to configure Business Space is with the Deployment Environment Configuration wizard. For more information, see "Configuring Business Space using the Deployment Environment Configuration wizard."

If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, Representational State Transfer (REST) service endpoints are configured and enabled automatically. For other environments, use the REST services administrative console page to configure the REST servicess. If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets. You must register the REST endpoints so that Business Space associates widgets with the endpoints and the widgets appear in the palette for use.

If you are using deployment manager and custom profiles, you can use the administrative console to configure Business Space.

After your original setup work on the Profile Management Tool or the administrative console, you must also configure the database tables for Business Space. For more information, see "Configuring Business Space database tables."

No matter what tool you used to configure Business Space, you must make sure Business Space works with the security for your environment. For more information, see "Setting up security for Business Space."

Business Space is built on Lotus Mashups technology. For frequently asked questions and general troubleshooting information about Lotus Mashups, see http://www.lotus.com/ldd/mashupswiki.nsf/xpViewCategories.xsp?lookupName=Troubleshooting&SessionID=CDFG4HK6EQ.

What to do next

After you have installed and configured Business Space, users of your runtime environment can open it from the following URL: http://*host*:*port*/BusinessSpace, where *host* is the name of the host where your server is running and *port* is the port number for your server.

Configuring Business Space using the Profile Management Tool

You can configure Business Space powered by WebSphere using the Profile Management Tool.

About this task

You can start the Profile Management Tool after product installation. In addition, you can use the Profile Management Tool capabilities from the command line by using the manageprofiles command-line utility parameter -configureBSpace after product installation. In both situations, Business Space is installed with the same database product as the database product you designate for the Common database. If you selected a database that is not supported with Business Space, the Profile Management Tool configures Business Space with the Derby Embedded database.

Process Server / ESB The Profile Management Tool is not available with WebSphere Process Server for z/OS and WebSphere Enterprise Service Bus for z/OS. For those products, configure Business Space using the administrative console.

For all products, for deployment manager and custom profiles, you can use the administrative console or the Deployment Environment Configuration wizard. See "Configuring Business Space using the administrative console" or "Configuring Business Space using the Deployment Environment Configuration wizard". If you use the Profile Management Tool to create a deployment manager and custom profiles (managed nodes) with the **Deployment environment** profile creation option, Business Space is configured automatically with your deployment environment, but you must manually run scripts to configure the database tables.

For more advanced configuration options on a stand-alone server profile, you must use pages on the administrative console to configure Business Space. For example, if you want to designate a data source that is different than the database you selected for your profile (the WebSphere Business Monitor database, the WebSphere Business Compass database, or the WebSphere Process Server common database), you must use the administrative console to configure Business Space.

If you have decided to use these more advanced configuration options, which require using the administrative console, make sure to complete the following steps:
* When you create the stand-alone server profile using the Profile Management Tool, use the **Advanced** profile creation option and clear the **Configure Business Space** check box, so you can configure Business Space later using the administrative console.
* See "Configuring Business Space using the administrative console."

If you are configuring a stand-alone server, complete step 1. If you are configuring a deployment environment, complete step 2.

Procedure

1. For a stand-alone server, start the Profile Management Tool, select the **Stand-alone server profile** option and complete the following steps.

   a. Complete one of the following steps on the Profile Creation Options page:

      - Select the **Typical** profile creation option if you want to accept a default installation and configuration of Business Space using the Derby Embedded database.

      - Select the **Advanced** option if you want to configure advanced options for the profile you are creating. Then on the Business Space Configuration page, make sure that the **Configure Business Space** check box is selected. If you want to configure Lotus Webform Server to work with Human Task Management widgets in Business Space, select the **Configure Lotus Webform Server** check box and enter the Webform Server translator and installation root.

      Business Space is configured with your product data source. If you are using the Profile Management Tool with IBM WebSphere Dynamic Process Edition, Business Space is configured with the WebSphere Process Server data source.

   b. When you designate the host name for your profile, use a fully qualified host name.

   c. On the Database Design page, you have the option of using a database design file that you have created using the database design tool that contains all database configuration for your product, including the database configuration information for Business Space.

   d. Complete the profile creation using the Profile Management Tool. Business Space is installed. It is configured for the same database product as the that you designated for the Common database (or with Derby Embedded if the database product is not supported).

   e. If the database is remote, you must configure the database tables after running the Profile Management Tool. See "Configuring Business Space database tables."

2. For a deployment environment, start the Profile Management Tool, select the **Deployment manager profile** or **Custom profile** option and complete the following steps.

   a. On the Profile Creation Options page, select the **Deployment environment** option to configure each profile with customized configuration values and use it in a deployment environment based on a supplied pattern.

   b. Follow the Profile Management Tool steps to create a deployment manager profile and custom profiles (managed nodes).

   c. After all the custom nodes are federated, run scripts to configure the database tables manually. See "Configuring Business Space database tables."

What to do next

Note: If your product database is an Oracle database, Business Space is configured with the Profile Management Tool or the manageprofiles command-line utility to use the same database, with the default schema IBMBUSSP, and the default password that you input during profile creation. If you want to use a different password for the IBMBUSSP user name, you must use the administrative console to updated JDBC Resources: Find the data source jdbc/mashupsDS. Modify the value of the authentication alias to make it match the password of the Business Space schema name. Save your changes and restart the server.

Before using Business Space, set up security that you need to use with Business Space and the widgets your team is using. For more information, see "Setting up security for Business Space."

Note: Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. If the REST service connections are timing out, update the following settings. By default, the socket-timeout value is set to 30 seconds. Change it to an appropriate value for your situation.

1. Open the file *profile_root*/BusinessSpace/*node_name*/*server_name*/ mm.runtime.prof/config/proxy-config.xml

2. Change the proxy:value for socket-timeout. The time is specified in milliseconds.

   ```
   <proxy:meta-data>
    <proxy:name>socket-timeout</proxy:name>
    <proxy:value>30000</proxy:value>
   </proxy:meta-data>
   ```

3. Run the updateBlobConfig command using the wsadmin scripting client, designating the following parameters: **-serverName** and **-nodeName** for a stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the value of the path for the proxy-config.xml file, and **-prefix** with the value Mashups_.

4. Restart the mm_was_*node_server* application from administrative console or the entire server application.

Configuring Business Space as part of the Deployment Environment Configuration wizard

Business Space configuration and Representational State Transfer (REST) service configuration for widgets in Business Space are automatically included in the Deployment Environment Configuration wizard. You can decide which REST services to configure.

Before you begin

Before you begin this task, you must complete the following tasks:
- Install your product.
- Create a profile, making sure to designate a fully qualified host name for the profile.
- Enable security, if you want to set up a secured environment for Business Space.

About this task

If you are setting up deployment manager and custom profiles, this method is the simplest way to configure Business Space.

Procedure

1. On the administrative console, click **Servers** → **Deployment Environments** → **New**. A series of pages in the wizard guides you through the process of creating your deployment environment.

2. Either define the new deployment environment or import a file that contains deployment environment definitions. You can create a deployment environment based on one of the IBM-supplied patterns or you can create a custom deployment environment.

3. On the Deployment Environment Patterns page, select one of the deployment environment patterns.

4. On the Select Nodes page, designate the nodes to participate in your deployment environment.

5. On the Clusters page, specify the number of cluster members from each node to assign to specific deployment environment functions.

6. On the Database page, configure the data source for Business Space, one of the components listed in the table. You can edit the description, test the connection, and set the database product you want to use for the Provider. You cannot select the **Create tables** check box on this page for Business Space. Database tables must be configured manually for Business Space. The database product list contains all databases supported by each component.

7. On the Security page, configure the authentication aliases WebSphere uses when accessing secure components. The authentication alias user name and password can be changed on this page. These aliases are used to access secure components but do not provide access to data sources.

8. For WebSphere Process Server configuration, supply information required to configure the application deployment target to support the deployment of the Business Process Choreographer components. Specify the context roots, security, and human task manager mail session values the wizard uses to configure Business Process Choreographer for this deployment environment.

9. For WebSphere Process Server configuration, configure the business rules manager to run on the cluster or server.

10. On the REST Services page, configure the services for the widgets you want available on Business Space for your runtime environment.

   - Type the port number and the host or virtual host that a client needs to communicate with the server or cluster. In a clustered environment, this is typically the load-balancing server host name and port.
   - If you leave the host and port fields empty, the values default to values of an individual cluster member host and its HTTP port. For a load-balanced environment, you must later change the default values to the virtual host name and port of the load-balancing server. Make sure to designate a fully qualified host name.
   - Set the description for the widgets if needed.

   .

11. On the next page, click **Finish** or **Finish and Generate Environment**.

12. Run the scripts to configure the database tables for Business Space before starting the deployment environment or the clusters. For more information, see "Configuring Business Space database tables."

What to do next

Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. If the REST service connections are timing out, update the following settings. By default, the socket-timeout value is set to 30 seconds. Change it to an appropriate value for your situation.

1. Open the file *profile_root*/BusinessSpace/*node_name*/*server_name*/
   `mm.runtime.prof/config/proxy-config.xml`
2. Change the `proxy:value` for `socket-timeout`. The time is specified in
   milliseconds.

   ```
   <proxy:meta-data>
    <proxy:name>socket-timeout</proxy:name>
    <proxy:value>30000</proxy:value>
   </proxy:meta-data>
   ```
3. Run the updateBlobConfig command using the wsadmin scripting client,
   designating the following parameters: **-serverName** and **-nodeName** for a
   stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the
   value of the path for the `proxy-config.xml` file, and **-prefix** with the value
   `Mashups_`.
4. Restart the mm_was_*node_server* application from administrative console or the
   entire server application.

Configuring Business Space for network deployment environments

If you have a distributed or network deployment environment, configure Business
Space using the administrative console or commands.

About this task

If you are using deployment manager and custom profiles, you must configure
Representational State Transfer (REST) endpoints, configure Business Space,
register the REST endpoints, and configure database tables.

Configuring REST services

If you have a stand-alone server environment or you are using the Deployment
Environment wizard to configure your runtime environment, Representational
State Transfer (REST) services are configured and enabled automatically. For other
environments, use the administrative console to configure the REST services.

About this task

If you want widgets to be available in Business Space, you must configure the
REST services for those widgets. Later you must register the REST endpoints so
that Business Space associates widgets with the endpoints and the widgets appear
in the palette for use.

You can configure all REST services for a specific server or cluster. Or, you can
select individual services to configure. You can manage individual service
configuration by viewing all services for a service provider or by viewing all
services for your environment.

Configuring all REST services on the administrative console:

Configure all Representational State Transfer (REST) services for your environment
by using the REST service administrative console page.

Before you begin

Before you complete this task, you must have installed your WebSphere business
process management product.

About this task

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the administrative console page allows you to configure REST services for all of your product's widgets in Business Space. On the REST Services page, you can view all services for your environment and enable or disable each service individually.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see "Enabling Business Space widgets for multiple endpoints."

Procedure

1. Click **Services** ⇒ **REST services** ⇒ **REST services**.

   The REST Services page opens, displaying all REST services in your environment.
2. For the **Scope section**, designate all to view all REST services in your environment, or select a server or cluster where you have REST services enabled.
3. In the table that lists the REST services for the provider, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.
4. For each individual service that you want to enable, type a meaningful description in the **Description** column.
5. Click **OK** to commit the changes to the services.

What to do next
- Configure Business Space.
- Configure the database tables (if you are using a remote database or a network deployment environment).
- Register REST service endpoints.
- For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.
- Set up security for Business Space.

Configuring REST services in a service provider:

Configure Representational State Transfer (REST) services in a service provider by using the REST service providers configuration administrative console page.

Before you begin

Before you complete this task, you must have installed your WebSphere business process management product.

About this task

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the administrative console allows you to configure REST services for all of your product's widgets in Business Space. On the REST service providers configuration administrative console page, you can view all services for a selected service provider and enable or disable each service individually. This page allows you to manage individual service configuration by working with all services for a service provider. If you prefer to manage REST services by your server or cluster (or by business processes or human task components), use the REST Services administrative console page.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see "Enabling Business Space widgets to work with multiple endpoints."

Procedure

1. Click **Services** → **REST services** → **REST service providers** → .

   The REST service providers page opens, displaying all REST service providers.

2. Click a provider link to configure the services for the group of REST services managed by that provider.

   The REST service providers configuration page opens, displaying all REST services in the provider.

3. Select a **Protocol** from the list for all REST services that you want to configure so they are available in Business Space. Configure a full URL path by selecting either **https://** or **http://** and then completing the **Host Name or Virtual Host in a Load-Balanced Environment** and **Port** fields. Use a fully qualified host name.

   If you want REST requests to go directly to the application server, type the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, type the host name and port of the proxy server or HTTP server that you have already set up. In an environment with a load balancer or proxy server between the browser and the Business Space and REST services, make sure that what you designate for the protocol, host, and port matches the browser URL for accessing Business Space.

4. In the table that lists the REST services for the provider, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.

5. For each individual service that you want to enable, type a meaningful description in the **Description** column.

6. Click **OK** to commit the changes to the services.

What to do next

- Configure Business Space.
- Configure the database tables (if you are using a remote database or a network deployment environment).
- Register REST service endpoints.

- For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.
- Set up security for Business Space.

Configuring REST services for a server, cluster, or component:

Configure Representational State Transfer (REST) services for a server, cluster or a component by using the REST Services administrative console page.

Before you begin

Before you complete this task, you must have installed your WebSphere business process management product.

About this task

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the REST Services administrative console page allows you to configure services for a server, a cluster, or a component.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see "Enabling Business Space widgets to work with multiple endpoints."

Procedure

1. Click one of the following.
   - For REST services on a server, click: **Servers** → **Server Types** → **WebSphere application servers** → *name_of_server* → **Business Integration** → **REST Services**
   - For REST services on a cluster, click: **Servers** → **Clusters** → **WebSphere application server clusters** → *name_of_cluster* → **Business Integration** → **REST Services**
   - For business process REST services on a server, click: **Servers** → **Server Types** → **WebSphere application servers** → *name_of_server* → **Business Integration** → **Business Flow Manager** → **REST Services**
   - For business process REST services on a cluster, click: **Servers** → **Clusters** → **WebSphere application server clusters** → *name_of_cluster* → **Business Integration** → **Business Flow Manager** → **REST Services**
   - For human task REST services on a server, click: **Servers** → **Server Types** → **WebSphere application servers** → *name_of_server* → **Business Integration** → **Human Task Manager** → **REST Services**
   - For human task REST services on a cluster, click: **Servers** → **Clusters** → **WebSphere application server clusters** → *name_of_cluster* → **Business Integration** → **Human Task Manager** → **REST Services**

   The REST Services page appears, displaying all default REST services that you can configure for Business Space widgets for use with your product or

component (Business Flow Manager or Human Task Manager). If a REST service has already been configured, you see a message displayed.

2. Select a **Protocol** from the list for all REST services that you want to configure so they are available in Business Space. Configure a full URL path by selecting either **https://** or **http://** and then completing the **Host Name or Virtual Host in a Load-Balanced Environment** and **Port** fields. Use a fully qualified host name.

   If you want REST requests to go directly to the application server, type the application server host name and port. If you want REST requests to go to a proxy server or HTTP server that sits in front of one or more application servers, type the host name and port of the proxy server or HTTP server that you have already set up. In an environment with a load balancer or proxy server between the browser and the Business Space and REST services, make sure that what you designate for the protocol, host, and port matches the browser URL for accessing Business Space.

3. In the table of REST services, in each row, select the **Enabled** check box if you want to enable the individual REST service, or clear the **Enabled** check box if you want to disable the individual REST service.

4. In the table of REST services, type a meaningful description for each of the REST services in the **Description** field.

5. Click **OK** to commit the changes to the services.

   To modify the REST service configuration at later time, you can come back to the REST Services page or you can use other administrative console pages to manage the configuration of REST service endpoints. The REST service providers page allows you to select service provider that you want to configure. The REST services page accessed from **Services → REST services** allows you to configure all REST services in your environment.

What to do next

- Configure Business Space.
- Configure the database tables (if you are using a remote database or a network deployment environment).
- Register REST service endpoints.
- For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.
- Set up security for Business Space.

Configuring REST services using the command line:

All widgets required for your product are installed with Business Space powered by WebSphere. The Representational State Transfer (REST) services for widgets must be configured, enabled, and registered with Business Space before your team can use the widgets in Business Space. If you do not use the REST Services administrative console page, use the updateRESTGatewayService command.

Before you begin

Before you complete this task, you must have installed your WebSphere business process management product.

For WebSphere Process Server, if you have configured Business Process Choreographer, the Human Task Management REST services are already

configured. However the REST Services Gateway application, which is a service provider for other REST services, must be configured with the updateRESTGatewayService command.

About this task

The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the REST Services administrative console page or the updateRESTGatewayService command allows you to configure services for REST application programming interfaces (APIs) for all of your product's widgets in Business Space.

You also must register the REST endpoints with Business Space. Then Business Space associates widgets with these endpoints, and the widgets appear in the palette for use.

If you want to configure multiple instances of the same REST service endpoint, you must manually edit the endpoints file and the widgets metadata file. For more information, see "Enabling Business Space widgets for multiple endpoints."

Procedure
1. Open a command window.

   The wsadmin command can be found in the *profile_root*/bin directory for a stand-alone server environment, or in the *deployment_manager_profile_root*/ bin directory for a network deployment environment.
2. At the command prompt, type the wsadmin command to start the wsadmin environment.
3. Use the updateRESTGatewayService command to configure REST services specifying the cluster or the server and node. The **-enable** parameter is optional, and if not specified, defaults to true.
4. Run the save command.

Example

The following example uses Jython to run the updateRESTGatewayService command and then save the changes. It configures the REST services on a cluster.
```
AdminTask.updateRESTGatewayService('[-clusterName
 cluster_name]')
AdminConfig.save()
```

The following example uses Jacl:
```
$AdminTask updateRESTGatewayService {-clusterName
 cluster_name}
$AdminConfig save
```

What to do next
• Configure Business Space.
• Configure the database tables (if you are using a remote database or a network deployment environment).
• Register REST service endpoints.
• For multiple instances of service endpoints, for example if you have partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster.

- Set up security for Business Space.

Configuring Business Space and registering REST endpoints on the administrative console

You can install and configure Business Space powered by WebSphere using the administrative console.

Before you begin

Before you begin this task, you must complete the following tasks:
- Install the product software and created a profile. When you install your product, Business Space files are included with the installation for the profiles that you set up. Your profile is not configured for Business Space until you explicitly configure Business Space on the profile.
- Configure Business Process Choreographer for WebSphere Process Server runtime environments that need the Human Task Management widgets. For more information, see "Configuring Business Process Choreographer" in the WebSphere Process Server documentation.
- Enable security, if you want to set up a secured environment for Business Space.
- Configure Representational State Transfer (REST) services. If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, the REST service endpoints are configured and enabled automatically. For other environments, use the REST services administrative console page to configure the REST services. If you want widgets to be available in Business Space, you must configure the REST services for those widgets. On the Business Space Configuration administrative console page, you register the REST endpoints so that Business Space associates widgets with the endpoints and the widgets appear in the palette for use.
- If you want to configure Business Space on a server or cluster using a different data source than the product data source: Create the data source in the server or cluster scope with the correct JNDI name of jdbc/mashupDS before configuring Business Space using the administrative console.
- For Oracle, to use a different schema for the Business Space tables than the one used by the product database, complete the following steps to create a data source manually before you open the Business Space Configuration page:
  - Create the schema using the database product software.
  - Use the administrative console to configure the JDBC provider.
  - Use the administrative console to create a data source with the JNDI name of jdbc/mashupDS at the server or cluster scope, depending on your environment.
  - Use the administrative console to create an authentication alias. Set the user name to the schema you created and set the authentication according to your Oracle setup.
  - Set the authentication alias on the data source.

About this task

If you are using deployment environments or other advanced profile configuration, you must use the administrative console to configure Business Space to work with your runtime environment. Business Space is a browser-based graphical user interface for the business users of the application that is running with the profile you set up. In Business Space, you and your application users can customize content from products in the WebSphere business process management portfolio.

Procedure

1. Ensure that the administrative console is running.
2. In the navigation pane click **Servers** → **Server Types** → **WebSphere application servers** or **Servers** → **Clusters** → **WebSphere application server clusters**.
3. Select the name of your server or cluster target.
4. On the Configuration page, under **Business Integration**, click **Business Space Configuration**. The Business Space Configuration page appears. If Business Space has already been configured, you can view this page but cannot edit the fields.
5. Select the **Install Business Space service** check box.
6. In the **Database schema name** box, type the name of the database schema you want to use for the Business Space database.

   Note: In Oracle, the schema is the same as the user name set on the authentication alias on the data source.
7. If no data source is designated in the **Existing Business Space data source** field, go to **Create Business Space data source using:** and select a data source that connects to the database you want to use with Business Space.

   Designating a data source under **Create Business Space data source using:** creates a data source for Business Space with a JNDI name of jdbc/mashupDS that is modeled on the data source you selected.

   The Business Space data source is created on the server or cluster on which you are configuring Business Space, even if the product data source is on a different server or cluster.

   Note: If you do not see an existing data source that you want to use, you must cancel the Business Space Configuration page, set up the database and the data source that you want to use, and then restart the Business Space Configuration page to complete the configuration. For more information, see the Before you begin section.
8. Click **OK**.
9. To register the proper deployment target (cluster or server) for the system Representational State Transfer (REST) endpoints for each of the widgets you are using in Business Space, click **REST service endpoint registration**. The target that you select for a REST service endpoint type can set the scope of the data displayed in some widgets. Or, you might want to select a particular cluster or server for better performance or availability. If you do not specify the target, the REST endpoint of this type is not registered with Business Space, and any widgets that need the REST service endpoint of this type will not be visible in Business Space.
10. Save the configuration.
11. Run the scripts to configure the database tables for Business Space before starting the deployment environment or the clusters. The scripts were generated when you completed the configuration. For more information, see Configuring Business Space database tables.

What to do next

Note: If you are using Oracle, the password of the authentication alias of the Business Space data source is set to same as the schema name of Business Space. The default value of the schema is IBMBUSSP. When you configure Business Space, you can specify a different schema on the administrative console or in the command line. In that case, the default password is the same as the schema you

specify. If you want to use a different password for the Business Space user name, you must use the administrative console to updated JDBC Resources: Find the data source jdbc/mashupsDS. Modify the value of the authentication alias to make it match the password of the Business Space schema name. Save your changes and restart the server.

Note: Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. If the REST service connections are timing out, update the following settings. By default, the socket-timeout value is set to 30 seconds. Change it to an appropriate value for your situation.

1. Open the file *profile_root*/BusinessSpace/*node_name*/*server_name*/ `mm.runtime.prof/config/proxy-config.xml`
2. Change the `proxy:value` for `socket-timeout`. The time is specified in milliseconds.

   ```
   <proxy:meta-data>
    <proxy:name>socket-timeout</proxy:name>
    <proxy:value>30000</proxy:value>
   </proxy:meta-data>
   ```
3. Run the updateBlobConfig command using the wsadmin scripting client, designating the following parameters: **-serverName** and **-nodeName** for a stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the value of the path for the `proxy-config.xml` file, and **-prefix** with the value `Mashups_`.
4. Restart the mm_was_*node_server* application from administrative console or the entire server application.

Configuring Business Space using the command line

You can set up and configure Business Space powered by WebSphere using the wsadmin command. You can use the wsadmin command to perform the same configuration of Business Space that you can perform in the administrative console.

Before you begin

Before you begin this task, you must complete the following tasks:
- Install the product software and create a profile. When you install your product, Business Space files are included with the installation for the profiles that you set up. Your profile is not configured for Business Space until you explicitly configure Business Space on the profile.
- Configure Business Process Choreographer for WebSphere Process Server runtime environments that need the Managing Tasks and Workflows widgets. For more information, see "Configuring Business Process Choreographer" in the WebSphere Process Server documentation.
- Enable security, if you want to set up a secured environment for Business Space.
- Configure Representational State Transfer (REST) services. If you have a stand-alone server environment or you are using the Deployment Environment wizard to configure your runtime environment, the REST service endpoints are configured and enabled automatically. For other environments, use the REST services administrative console page to configure the REST services. If you want widgets to be available in Business Space, you must configure the REST service endpoints for those widgets. You must register the REST endpoints so that Business Space associates widgets with the endpoints and the widgets appear in the palette for use.

- If you want to configure Business Space on a server or cluster using a different data source than the product data source: Create the data source in the server or cluster scope with the correct JNDI name of jdbc/mashupDS before configuring Business Space (before running the configureBusinessSpace command).
- For Oracle, to use a different schema for the Business Space tables than the one used by the product database, complete the following steps to create a data source manually before you run the commands to install and configure Business Space in the procedure below:
  - Use the administrative console to configure the JDBC provider.
  - Use the administrative console to create a data source with the JNDI name of jdbc/mashupDS at the server or cluster scope, depending on your environment.

About this task

You can use the command line to configure Business Space if you want to write scripts instead of using the administrative console to configure Business Space.

If you are not sure whether Business Space is already configured, you can run the getBusinessSpaceDeployStatus command to check whether Business Space is configured on a server, cluster, or cell. For more information about that command, see "getBusinessSpaceDeployStatus command."

Procedure

1. Open a command window.

   The wsadmin command can be found in the *profile_root*/bin directory for a stand-alone server environment, or in the *deployment_manager_profile_root*/bin directory for a network deployment environment.

2. At the command prompt, type the wsadmin command to start the wsadmin environment.

3. Use the installBusinessSpace command to install the Business Space enterprise archive (EAR) files in your runtime environment.

4. Use the configureBusinessSpace command to configure the data source for Business Space and copy the scripts that configure the database tables to *profile_root*/dbscripts/BusinessSpace/*node_name_server_name*/ *database_type*/*database_name* for a stand-alone server or *profile_root*/ dbscripts/BusinessSpace/*cluster_name*/*database_type*/*database_name* for a cluster. You must run the scripts that configure the database tables. For more information about the scripts, see "Configuring Business Space database tables."

   If you are using a database design file for database configuration, you can use the **-bspacedbDesign** parameter to designate that file when you run the configureBusinessSpace command.

5. After each command, run `AdminConfig.save(` (Jython) or `$AdminConfig save` (Jacl).

6. Run the scripts to configure the database tables for Business Space before starting the deployment environment or the clusters. For more information, see Configuring Business Space database tables.

Results

Configuring Business Space sets up a browser-based graphical user interface for the business users of your application that is running with the profile you set up. In Business Space, you and your application users can customize content from

products in the WebSphere business process management portfolio.

Example

The following example uses Jython to run the installBusinessSpace and configureBusinessSpace commands to install the EAR files and configure the data source for Business Space on a cluster. The example designates the schema and the product database to use with Business Space when multiple products are installed. In a situation where both WebSphere Process Server and WebSphere Business Monitor are installed, this example creates a Business Space data source using the properties of the WebSphere Process Server data source.

```
AdminTask.installBusinessSpace('[-clusterName myCluster -save
 true]')

AdminTask.configureBusinessSpace('[-clusterName
 myCluster -schemaName mySchema -productTypeForDatasource
 WPS -save true]')
```

The following example uses Jacl:

```
$AdminTask installBusinessSpace {-clusterName myCluster -save
 true}

$AdminTask configureBusinessSpace {-clusterName
 myCluster -schemaName mySchema -productTypeForDatasource
 WPS -save true}
```

What to do next

Note: If you are using Oracle, the password of the authentication alias of the Business Space data source is set to same as the schema name of Business Space. The default value of the schema is IBMBUSSP. When you configure Business Space, you can specify a different schema on the administrative console or in the command line. In that case, the default password is the same as the schema you specify. If you want to use a different password for the Business Space user name, you must use the administrative console to updated JDBC Resources: Find the data source jdbc/mashupsDS. Modify the value of the authentication alias to make it match the password of the Business Space schema name. Save your changes and restart the server.

To enable Business Space for your runtime environment, you must perform the following steps after configuring Business Space from the command line.

- Register the endpoints with the registerRESTserviceEndpoint command.
- Set up security that you need to use with Business Space and the widgets your team is using. For more information, see "Setting up security for Business Space."

Note: Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. If the REST service connections are timing out, update the following settings. By default, the socket-timeout value is set to 30 seconds. Change it to an appropriate value for your situation.

1. Open the file *profile_root*/BusinessSpace/*node_name*/*server_name*/ mm.runtime.prof/config/proxy-config.xml
2. Change the `proxy:value` for `socket-timeout`. The time is specified in milliseconds.

```
<proxy:meta-data>
 <proxy:name>socket-timeout</proxy:name>
 <proxy:value>30000</proxy:value>
</proxy:meta-data>
```

3. Run the updateBlobConfig command using the wsadmin scripting client, designating the following parameters: **-serverName** and **-nodeName** for a stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the value of the path for the `proxy-config.xml` file, and **-prefix** with the value `Mashups_`.

4. Restart the mm_was_*node_server* application from administrative console or the entire server application.

Configuring Business Space database tables

You can manually install database tables for Business Space powered by WebSphere on a remote database server with scripts that are generated by the installation program. If you are using a deployment environment, or your database is remote, you must install these tables after configuring Business Space.

Before you begin

Before you complete this task, you must have completed the following tasks:
• Installed the product.
• Created profiles and configured servers or clusters for Business Space.
• For Oracle: created the database.
• For Microsoft SQL Server: set SQL Server instance authentication. The SQL Server JDBC driver supports mixed authentication mode only. Therefore, when the SQL Server instance is created, the authentication must be set to **SQL Server and Windows**.
• For all databases, make sure that the database is installed using a UTF-8 Universal character set if you want to use Business Space in your environment.
• Made sure that your application server with Business Space is stopped.

   Monitor   **Process Server / ESB** If you are using DB2 for z/OS and the required resources have not already been set up as part of the core product installation, complete the following additional items before you begin this task:
• Create a TEMP database and a TEMP table space to contain the declared temporary tables for processing scrollable cursors.
• Create a dedicated STOGROUP to contain the Business Space data.

   Monitor   **Process Server / ESB** For DB2 for z/OS, if you want to use a different storage group (for example, if you don't want Business Space database tables to be added to the same database and storage group as the common database), you must edit and run the `createStorageGroup.sql` script after you configure Business Space and before you configure the Business Space database tables.
• Edit the `createStorageGroup.sql` file, available in the following location: *profile_root*/dbscripts/BusinessSpace/*node_name_server_name/database_type*/*database_name* for a stand-alone server, or *profile_root*/dbscripts/BusinessSpace/*cluster_name/database_type/database_name* for a cluster, where *database_type* is either DB2zOSV8 or DB2zOSV9.
• Change the VCAT value from @VCAT@ to the name or alias of the catalog of the integrated catalog facility for the storage group to use.

If you are using DB2 V9.x, and you would like performance improvements, edit the createTableSpace.sql file. The createTableSpace.sql file is available in *profile_root*/dbscripts/BusinessSpace/*node_name_server_name*/*database_type*/ *database_name* for a stand-alone server, or *profile_root*/dbscripts/BusinessSpace/ *cluster_name*/*database_type*/*database_name* for a cluster.

- Change IMMEDIATE SIZE 8000 PAGESIZE 32K to IMMEDIATE SIZE 8000 AUTOMATIC PAGESIZE 32K.
- Add the line PREFETCHSIZE AUTOMATIC after EXTENTSIZE 16 under both CREATE SYSTEM TEMPORARY TABLESPACE @TSDIR@TMPTP and CREATE REGULAR TABLESPACE @TSDIR@REGTP.

About this task

The configBusinessSpaceDB script sets up tables for Business Space with a specific database. If you want to create tables on an existing database other than the specific one, use the createDBTables script with your product.

Procedure

1. Make sure that you are using a user ID with sufficient authority to create tables.
2. Locate the script in the profile you most recently configured, and save it to a location on the same system with the database.
   - For all databases except DB2 for z/OS, locate the configBusinessSpaceDB.bat or configBusinessSpaceDB.sh script.
   - **Process Server / ESB** For WebSphere Process Server for z/OS and WebSphere Enterprise Service Bus for z/OS, locate the createDB.sh script if you want to configure the Business Space database tables with all other database objects.
   - **Monitor** **Process Server / ESB** For DB2 for z/OS, if you don't run the createDB.sh script, you must run the Business Space files individually. Locate createStorageGroup.sql, createDatabase.sql, createTablespace.sql, createTables_BusinessSpace.sql, and createTable.sql.

   By default, the scripts are located in the following directory: *profile_root*/dbscripts/BusinessSpace/*node_name_server_name*/ *database_type*/*database_name* for a stand-alone server, or *profile_root*/ dbscripts/BusinessSpace/*cluster_name*/*database_type*/*database_name* for a cluster. The updated scripts (with the information that you entered during profile creation) are located in the profile for the server or cluster that you most recently configured. If you used the Deployment Environment Configuration wizard, the scripts are located in the deployment manager profile. When configuring a remote database, copy the scripts from the system where your product is installed to a place on the remote system.
3. **Process Server / ESB** **For WebSphere Process Server for z/OS and WebSphere Enterprise Service Bus for z/OS:** If you are configuring DB2 for z/OS, you can use the createDB.sh script to configure the Business Space database tables with all other database objects in one database. For more information, see "Creating DB2 database objects using the createDB.sh script" in the WebSphere Process Server for z/OS documentation.
4. Open a command prompt and run one of the following commands, based on your platform.

For Derby, run the command in the default location (*profile_root*/dbscripts/ BusinessSpace/*node_name_server_name*/*database_type*/*database_name* for a stand-alone server).

For other database types, copy the folder with the batch files and scripts to the same location as your database and run the command there. Your user ID must have access to the command-line interpreter for the database type and have permission to run commands.

- **Linux** **UNIX** **On Linux, UNIX, and z/OS platforms:** `configBusinessSpaceDB.sh`

- **Windows** **On Windows platforms:** `configBusinessSpaceDB.bat`

For Derby, DB2 and SQL Server, use the optional **-createDB** parameter if you want to create a different database instead of using the existing database.

Note: When using SQL Server, you see the following warning statements in the `systemout.log` file after running the database script: `... Warning! The maximum key length is 900 bytes ....` If you are using the federated repositories as a user registry, you can ignore the warnings. If you are using the stand-alone LDAP registry, ensure that all the user distinguished name (DN) entries in your organization are less than the 131 character limit. If any of the user DN entries exceed 131 characters, you must change the user account registry to the federated repositories option.

For z/OS, run the following files in order:
- createStorageGroup.sql
- createDatabase.sql
- createTablespace.sql
- createTables_BusinessSpace.sql
- createTable.sql

5. **Linux** **UNIX** **Windows** For DB2 and DB2 for z/OS, bind the command-line interface to the Business Space database using the following commands:

    db2 connect to *database_name*

    db2 bind *DB2_installation_directory*\bnd\@db2cli.lst blocking all grant public

    db2 connect reset

where:

database_name is the name of the Business Space database

DB2_installation_directory is the directory where DB2 is installed

What to do next

- Update the endpoints for widgets that you want to be available in Business Space.
- Set up security for Business Space and the widgets that your team is using.

Registering Business Space widget REST service endpoints using the command line

If you configure Business Space using the administrative console, you must register Representational State Transfer (REST) endpoints so that your team can use the widgets in Business Space. If you do not register your endpoints on the

administrative console using the Business Space Configuration and the System
REST service endpoint registration pages, you can register them using the
registerRESTServiceEndpoint command.

Before you begin

Before you complete this task, you must have completed the following tasks:
- Installed the product.
- Configured the REST services for the widgets that you are you using in Business
  Space by using the REST Services administrative console page or the
  updateRESTGatewayService command. If you have a stand-alone server
  environment or you are using the Deployment Environment wizard to configure
  your runtime environment, the REST services are configured and enabled
  automatically. You configure REST services for business processes and human
  tasks by configuring the Business Process Choreographer and the Human Task
  Manager container.
- Configured Business Space by using either the Business Space Configuration
  administrative console page or the installBusinessSpace and
  configureBusinessSpace commands.
- Configured the database tables (if you are using a remote database or a network
  deployment environment).

About this task

REST services are registered automatically if you have a stand-alone server
environment and you configured Business Space with the administrative console or
the Profile Management Tool, or if you used the Deployment Environment wizard
to configure your runtime environment. Otherwise, you must configure the REST
services and then register them.

The System REST service endpoint registration administrative console page or the
registerRESTServiceEndpoint command allows you to register endpoints for REST
services for all of your product's widgets in Business Space. Then Business Space
automatically associates widgets with these endpoints, and the widgets appear in
the Business Space palette for use.

The registerRESTServiceEndpoint command allows you to register a set of
endpoints for a given provider, a deployment target, or all unique endpoints in a
cell. This command registers the endpoints of the REST services that are in the
same cell as Business Space.

Procedure

1. Open a command window.

   The wsadmin command can be found in the *profile_root*/bin directory for a
   stand-alone server environment, or in the *deployment_manager_profile_root*/
   bin directory for a network deployment environment.
2. At the command prompt, type the wsadmin command to start the wsadmin
   environment.
3. Use the registerRESTServiceEndpoint command to register the Business Space
   endpoints for REST services for all your product's widgets.
4. After each command, run the save command.

Example

The following example uses Jython to run the registerRESTServiceEndpoint command and then save the changes. It registers all configured and enabled REST services on the cluster with Business Space.

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
 name_of_rest_services_cluster -businessSpaceClusterName
 name_of_business_space_cluster]')
AdminConfig.save()
```

where *name_of_rest_services_cluster* is the cluster name where REST services are configured and *name_of_business_space_cluster* is the cluster name where Business Space is deployed.

The following example uses Jacl:

```
$AdminTask registerRESTServiceEndpoint
{-clusterName name_of_rest_services_cluster
-businessSpaceClusterName name_of_business_space_cluster}
$AdminConfig save
```

where *name_of_rest_services_cluster* is the cluster name where REST services are configured and *name_of_business_space_cluster* is the cluster name where Business Space is deployed.

The **appName**, **webModuleName**, **type**, **version**, **nodeName**, **serverName**, or **clusterName** parameters are optional.

If you do not specify **type**, **appName**, and **webModuleName** parameters, all unique REST service endpoints configured on the deployment target are registered.

If you do not specify any of those parameters, all unique REST service endpoints configured on any deployment target are registered.

What to do next

Business Space uses a proxy component to connect to your REST services. In some cases, if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST services, depending on the performance of the REST service servers. If the REST service connections are timing out, update the following settings. By default, the socket-timeout value is set to 30 seconds. Change it to an appropriate value for your situation.

1. Open the file *profile_root*/BusinessSpace/*node_name*/*server_name*/ mm.runtime.prof/config/proxy-config.xml
2. Change the proxy:value for socket-timeout. The time is specified in milliseconds.

   ```
   <proxy:meta-data>
    <proxy:name>socket-timeout</proxy:name>
    <proxy:value>30000</proxy:value>
   </proxy:meta-data>
   ```

3. Run the updateBlobConfig command using the wsadmin scripting client, designating the following parameters: **-serverName** and **-nodeName** for a stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the value of the path for the proxy-config.xml file, and **-prefix** with the value Mashups_.
4. Restart the mm_was_*node_server* application from administrative console or the entire server application.

Configuring a proxy server or load balancer to use with Business Space

If you are using Business Space in an environment with a proxy server or a load-balancing server, you must set up your environment so that Business Space and widgets work properly.

About this task

In a Network Deployment, or clustered, environment, you might set up a proxy server or an HTTP server for security reasons and for workload balancing. Instead of incoming HTTP requests going directly to an application server, they go to a proxy server that can spread the requests across multiple application servers that perform the work.

You can use other routing servers in place of or in front of the proxy server, for example IBM HTTP Server.

Important: The proxy server (or an alternate routing server) is required for workload balancing HTTP requests across two or more cluster members. The proxy server allows clients to access the applications within this topology.

In an environment with a load balancer or proxy server between the browser and the Business Space and REST services, make sure that what you designate for the REST services protocol, host, and port matches the browser URL for accessing Business Space. On the REST service providers page on the administrative console, verify that for all providers, such as the Business Flow Manager and the Human Task Manager, have the correct protocol, host, and port. For more information about modifying the REST services, see Configuring REST services in a service provider.

If you use IBM HTTP Server, you must complete additional mapping steps to verify that modules are mapped to the web server and that the host aliases are configured.

If you use a reverse proxy setup for an HTTP server, you must map the URLs for Business Space and widgets.

Configuring IBM HTTP Server for Business Space:

If you use IBM HTTP Server, you must complete additional mapping steps so that Business Space works in your environment.

Before you begin

Before you configure IBM HTTP Server to work with Business Space, complete the following steps:
- Install IBM HTTP Server
- Make sure that Secure Sockets Layer (SSL) is enabled for IBM HTTP Server.
- Make sure that the web server definition for IBM HTTP Server has been added to the application server.

  During the installation of the IBM HTTP Server plug-in, a configure*Web_server* script is produced by the install process on the web server machine. The configure*Web_server* script is intended to map web application modules to the web server. Therefore, run this script after the generation of the deployment environment.

Procedure

1. Make sure that modules are mapped to the web server. For each of the applications required by Business Space, verify that the web server is one of the selected targets.

   a. Log in to the administrative console as an administrative user.

   b. Click **Applications** → **Application Types** → **WebSphere enterprise applications**.

   c. From the Enterprise Applications panel, click the name of the application.

      Check the following applications. You might have some or all applications in this list, based on which products you are using with Business Space.

      - **BPMAdministrationWidgets_*nodename_servername*** (for WebSphere Enterprise Service Bus and WebSphere Process Server)
      - **BusinessSpaceHelpEAR_*nodename_servername*** (for all products)
      - **BSpaceEAR_*nodename_servername***(for all products)
      - **BSpaceWebformsEnabler_*nodename_servername*** (for all products)
      - **HumanTaskManagementWidgets_*nodename_servername*** (for WebSphere Process Server and WebSphere Business Monitor)
      - **REST Services Gateway** (for all products)
      - **REST Services Gateway Dmgr** (for WebSphere Enterprise Service Bus and WebSphere Process Server)
      - **mm.was_*nodename_servername*** (for all products)
      - **WBMDashboardWeb_*nodename_servername*** (for WebSphere Business Monitor)
      - **wesbWidgets_*nodename_servername*** (for WebSphere Enterprise Service Bus)
      - **widgets_busleader_*nodename_servername*** (for WebSphere Business Compass)
      - **widgets_pubserver_*nodename_servername*** (for WebSphere Business Compass)
      - **widgets_fabric_*nodename_servername*** (for WebSphere Business Services Fabric)

   d. For each application, on the Configuration tab, under Modules, click **Manage Modules**.

   e. On the Manage Modules page for your application, make sure that the web server is one of the selected targets for each of your modules.

      - In the table, check the Server column for each module to make sure that the web server is one of the selected targets for each of your modules. For example, for the mm.was_*nodename_servername* application, look for the web server to be displayed in the Server column: **WebSphere:cell=qaxs41Cell02,node=qaxs41Node03,server=httpserver WebSphere:cell=qaxs41Cell02,cluster=Golden.WebApp**.

      - If you need to add the web server, select the check box next to the name of the module. Then, in the Clusters and servers list, use the Ctrl key to select multiple targets. For example, to have a web server serve your application, press the Ctrl key and then select the application server cluster and the web server together. Click **Apply**, **OK** and **Save** to save any changes.

2. Verify that the host name alias `default_host` contains the correct information for every cluster member, web server, or proxy server.

   a. Log in to the administrative console as an administrative user.

b. Click **Servers** → **Server Types** → **WebSphere application servers**.

c. For every cluster member, click the name of the application server to view the port number for the **WC_defaulthost** port name.

   - Under Communications, expand **Ports**.
   - For the port name **WC_defaulthost**, remember its port number.

d. From the left navigation area of the administrative console, click **Environment** → **Virtual hosts**.

e. Click the **default_host** name.

f. Under Additional Properties, click **Host Aliases**.

g. If the host name and port number for the cluster members is not displayed on the list, click **New** to add the missing entry to the list. The wildcard character * (asterisk) is supported for the host name.

h. If you add a new entry, click **Save** and **Synchronize**.

Mapping Business Space URLs for a reverse proxy server:

If you have a reverse proxy setup for your HTTP server, when you are configuring the HTTP server to work with Business Space, you must map the URLs for Business Space and the widgets that your team uses.

Procedure

1. Edit your HTTP server configuration file.
2. Map all of the URLs for Business Space and the widgets that your business users work with in the runtime solution.

   URLs for general Business Space framework (all products):
   - /BusinessSpace/*
   - /mum/*
   - /help/*
   - /BSpaceWebformsProxy/*
   - /themes/*

   Additional URLs for WebSphere Business Compass widgets:
   - /WBPublishingDRAFT/*
   - /BusinessLeader/*
   - /BusinessLeaderWidgets/*

   Additional URLs for WebSphere Business Services Fabric widgets:
   - /bpm/bslm/v1/*
   - /bpm/glossary/v1/*
   - /bpm/governance/v1/*
   - /bpm/bvars/v1/var/*
   - /rest/*

   Additional URLs for WebSphere Business Monitor widgets:
   - /BusinessDashboard/*
   - /DashboardABX/*
   - /monitorServerComponent/*
   - /mobile/*
   - /rest/*
   - /AlphabloxServer/*
   - /AlphabloxAdmin/*

- /AlphabloxTooling/*
- /BloxBuilder/*

Additional URLs for WebSphere Enterprise Service Bus widgets:

- /BSpaceWidgetsHM/*
- /rest/*
- /PolymorphicWidget/*
- /scaWidget/*
- /ServiceMonitorGraphWidget/*
- /StoreAndForward/*

Additional URLs for WebSphere Process Server widgets:

- /BSpaceWidgetsHM/*
- /SecurityManagerWidgets/*
- /BSpaceWidgetsBCM/*
- /rest/*
- /PolymorphicWidget/*
- /scaWidget/*
- /ServiceMonitorGraphWidget/*
- /StoreAndForward/*

Enabling Business Space widgets for cross-cell environments

You must manually edit endpoints files if Business Space is running on a different cell than where the Representational State Transfer (REST) services are running, or if widgets are on different cells than Business Space.

Before you begin

Before you complete this task, you must have completed the following tasks:
- Installed the product.
- Created profiles, and configured Business Space on a deployment target (server or cluster).
- Configured the database tables (if you are using a remote database or deployment environment).
- For WebSphere Business Compass, you must first update the Endpoints table in the WebSphere Business Compass database. Set the Server_Name column to the Business Space Internet Protocol and the Port column to the Business Space port.

About this task

All widgets required for your product are installed with Business Space, but you must configure and register the endpoints needed by the widgets before your team can use them in Business Space. You can configure and register the endpoints by using administrative console pages. However, if your product and REST services are installed on a different cell than Business Space, you must edit REST service endpoints files so that they access the REST services and your widgets work properly in Business Space.

Edit one or more of the following endpoint files, based on the products you have installed, and the widgets you are using with Business Space:
- WebSphere Business Compass: `pubserverEndpoints.xml` and `busLeaderEndpoints.xml`.

- WebSphere Business Monitor: `monitorEndpoints.xml`
- WebSphere Business Monitor with Alphablox: `monitorABXEndpoints.xml`
- WebSphere Business Services Fabric: `fabricEndpoints.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `bpmAdministrationEndpoints.xml` (for Administration widgets)
- WebSphere Process Server: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (for Administration widgets), `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `HumanTaskManagementEndpoints.xml` (for business processes and human tasks), `bspaceWFSEndpoints.xml` (for using Lotus Webform Server with Human Task Management widgets)
- All products: `wsumEndpoint.xml` (for user membership)

If you are an administrator, you can register endpoints and enable widgets by performing the following steps.

Procedure

1. Copy widgets from the cell where they were installed to the cell where Business Space is configured during product installation. Widgets can be found in the *install_root*`\BusinessSpace\widgets` directory and can be copied to a temporary folder.

2. Run the installBusinessSpaceWidgets command to install, deploy, and register designated widgets located in the *install_root*`\BusinessSpace\widgets` directory.

   a. Make sure the target server (for a stand-alone server environment) or the deployment manager (for a network deployment environment) is up and running, and on that profile, open a command window.

   The wsadmin command can be found at the `profiles\`*profile_name*`\bin` directory.

   b. At the command prompt, type the wsadmin command to start the wsadmin environment.

   c. Run the installBusinessSpaceWidgets command. For a clustered environment, specify the **-clusterName** parameter. For a stand-alone server environment, specify the **-serverName** and **-nodeName** parameters. Specify the **-widgets** parameter with the full path for the directory or file that contains the widgets.

3. Locate the endpoint files in the *install_root*`\BusinessSpace\registryData\`
   `endpoints` directory. For a cluster, use the deployment manager profile root. The file names all end with `Endpoints.xml` or `Endpoint.xml`.

4. For each endpoint file that you are configuring, make a backup copy.

5. Create the following directory on the deployment manager profile of the first cell (if it does not exist): *profile_root*`\BusinessSpace\registryData\` (where *profile_root* is typically *install_root*`\profiles\`*profile_name* or *install_root*`\pf\`*profile_name*) and copy the endpoint registration file to that directory.

6. Configure the endpoints as needed by editing the endpoint files. Each endpoint in the endpoint file is designated by a `<tns:Endpoint>` block. Identify the block that you want to change.

   Tip: If you do not intend to activate some endpoints, you can remove them from the file to prevent confusion.

The location identified by an endpoint is specified in `<tns:url>`. This value is a path in a web module, specified as a full or relative HTTP URL. By default, the URL is relative. Change it to a full URL path, for example, `https://`*virtualhost*`.com:`*virtualport*`/rest/bpm/htm` or `http://host1:9445/WBPublishingDRAFT/`, where the protocol, host, and port identify how the product web module can be accessed.

To locate the port number for the server, perform the following steps:

- Log in to the administrative console.
- Click **Servers** ‣ **Server Types** ‣ **WebSphere application servers**.
- Click the server for which you want to find the port number, and then expand the Ports section.

All applications use the same port as shown in either the **wc_defaulthost** (unsecured host) parameter or the **wc_defaulthost_secure** (secure host) parameter.

Note: If you are using an HTTP server to access your web modules for load balancing, use the host name and port settings of the HTTP server.

7. In the cell where the Business Space server is configured, run the updateBusinessSpaceWidgets command to update the endpoint URLs after you have modified the endpoints XML files.

a. For your profile, open a command window. The wsadmin command can be found at the `profiles\`*profile_name*`\bin` directory. For a clustered environment, run the command from the *deployment_manager_profile_root*`\bin` directory. For a stand-alone server environment, run the command from the *profile_root*`\bin` directory.

b. At the command prompt, type the wsadmin command to start the wsadmin environment.

c. Run the updateBusinessSpaceWidgets command. For a clustered environment, specify the **-clusterName** parameter. For a stand-alone server environment, specify the **-serverName** and **-nodeName** parameters. Specify the **-endpoints** parameter with the full path for the directory where the widget endpoint files are located or the full path to a specific endpoint file.

Example

The following example endpoint file is for WebSphere Business Monitor widgets.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- START NON-TRANSLATABLE -->
<tns:BusinessSpaceRegistry
 xmlns:tns="http://com.ibm.bspace/BusinessSpaceRegistry"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://com.ibm.bspace/BusinessSpaceRegistry
 BusinessSpaceRegistry.xsd ">

  <tns:Endpoint>
    <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/rest/</tns:url>
    <tns:description>Location of backing services for Monitor widgets
</tns:description>
  </tns:Endpoint>
```

```
</tns:BusinessSpaceRegistry>
<!-- END NON-TRANSLATABLE -->
```

What to do next
- After running the installBusinessSpaceWidgets command or the updateBusinessSpaceWidgets command, you must perform manual steps to update Business Space templates and spaces. For more information, see Updating Business Space templates and spaces after installing or updating widgets.
- For multiple instances of service endpoints, for example for partitioning of work on two clusters, and you want to have widgets showing data from each cluster, you must enable the additional widgets manually for each additional cluster. You must edit both the widget endpoints files and the widget catalog files. For more information, see Enabling Business Space widgets to work with multiple endpoints.
- If you have enabled security for your environment, you must make sure that it is set up properly to work with Business Space.

Enabling Business Space widgets to work with multiple endpoints

If you have one Business Space instance configured and you have a need to create another instance of the service endpoints in your environment, you must configure Business Space so that the widgets can display data from the multiple service endpoints. You must edit two files: the endpoints file, which registers endpoints with Business Space, and the widget catalog file, which contains definitions of widgets.

Before you begin

Before you complete this task, you must have completed the following tasks:
- Installed the product.
- Created a server or cluster and configured it for Business Space .
- Configured the database tables (if you are using a remote database or deployment environment).
- Configured the additional Representational State Transfer (REST) services for your additional widgets.

About this task

In a deployment environment, you can have partitioning of work. For example, you can have two clusters, one that processes accounting data and one that processes insurance data. However, a service endpoint serves only one cluster. To access both partitions of work from Business Space, you must register two separate widgets, one for each partition of work, so you can access them both from Business Space. For example, you could have an Account Human Task List widget and an Insurance Task List widget in the catalog (both with the same actual human task list code).

You must manually edit the endpoints file and the widget catalog file.

Widget endpoint files are bundled with each product and are added during the installation of the product. You must edit one or more of the following endpoint files, based on the products you have installed, and the widgets you are using with Business Space:

- WebSphere Business Compass: `pubserverEndpoints.xml` and `busLeaderWidgetEndpoints.xml`.
- WebSphere Business Monitor: `monitorEndpoints.xml`
- WebSphere Business Monitor with Alphablox: `monitorABXEndpoints.xml`
- WebSphere Business Services Fabric: `fabricEndpoints.xml`
- WebSphere Enterprise Service Bus: `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `bpmAdministrationEndpoints.xml` (for Administration widgets)
- WebSphere Process Server: `wpsEndpoints.xml`, `bpmAdministrationEndpoints.xml` (for Administration widgets), `wesbWidgetEndpoints.xml` (for Mediation Policy Administration, Service Browser, and Proxy Gateway widgets), `HumanTaskManagementEndpoints.xml` (for business processes and human tasks), `bspaceWFSEndpoints.xml` (for using Lotus Webform Server with Human Task Management widgets)
- All products: `wsumEndpoint.xml` (for user membership)

Widget catalog files contain the definition of widgets for your product. You must edit one or more of the following widget files, based on the products you have installed, and the widgets you are using with Business Space:

- WebSphere Business Compass: `catalog_pubserverWidgets.xml` and `catalog_busLeaderWidgets.xml`
- WebSphere Business Monitor: `catalog_WBMonitor.xml`
- WebSphere Enterprise Service Bus: `catalogProxyGateway.xml` and `catalog_ServiceAdmin.xml`
- WebSphere Process Server: `catalog_BPMAdministration.xml`, `catalog_BusinessRules.xml`, `catalog_ServiceAdmin.xml`, and `catalog_HumanTaskManagement.xml`
- WebSphere Business Services Fabric: `catalog_fabric.xml`

Both the endpoint files and the widget catalog files are located at *install_root*\BusinessSpace\registryData\. The endpoints files are located in the `endpoints` subdirectory, and the catalog files are located in the `catalogs` subdirectory.

The directory *install_root*\BusinessSpace\registryData\ contains endpoint and widget catalog template files for your product. You can copy the files that you need to use as a template and add your changes.

Procedure

1. In order to have multiple instances of a widget, you must install the applications that provide widgets with a unique application name and context root for each widget instance.

   a. Deploy the widget application on the Business Space deployment target (the same server or cluster on which the **BSpaceEAR_***server_node* application is running) for each widget instance. Depending on the products you are using, deploy one or more of the following Enterprise Archive (EAR) files:

      - BPMAdministrationWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus and WebSphere Process Server)

- HumanTaskManagementWidgets_*nodename_servername* (for WebSphere Process Server and WebSphere Business Monitor)
- WBMDashboardWeb_*nodename_servername* (for WebSphere Business Monitor)
- wesbWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus)
- widgets_busleader_*nodename_servername* (for WebSphere Business Compass)
- widgets_pubserver_*nodename_servername* (for WebSphere Business Compass)
- widgets_fabric_*nodename_servername* (for WebSphere Business Services Fabric)

   b. When deploying, update the application name and the web module context root names to a unique name. Take note of the context root names that you use.

2. Edit the new REST service endpoints for the additional application deployment targets (the server or cluster where the REST services application is deployed). Create an endpoints file to add service endpoints.

   a. Locate the endpoint files in the *install_root*\BusinessSpace\registryData\ endpoints directory. Copy the endpoints template file, and remove all the endpoints that you do not intend to change.

   b. Edit the endpoints file and add an additional service endpoint starting with `<tns:Endpoint>`, with a unique ID (`<tns:id>`) and the URL for the new endpoint (`<tns:url>`), but with the same version, and optionally all the locales as the original endpoint. The type (`<tns:type>`) must have the same value as the ID (`<tns:id>`). You can change the name and description, for example, `My team's insurance task list`.

   c. When adding endpoints, pay attention to the following information:
      - `<tns:id>`: The ID can be any string but must be unique for all registered endpoints. Ensure that this ID is unique when you are adding additional endpoints.
      - `<tns:type>`: The type must have the same value as `<tns:id>`.
      - `<tns:url>`: For the service endpoint, if the URL is relative, then it is assumed that the REST service endpoint is co-located with the Business Space server. If the URL is relative, make sure the URL is same as the context root you deployed, but with beginning and end directory indications, for example, `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`. If your endpoint is on a remote system, update this field with an absolute URL, but with an end directory indication.
      - `<tns:description>`: Type a meaningful description that further details the nature of the data set that this endpoint is working on. It could either be based on the cluster that is working on the data set or the nature of the data set, for example, `insurance claim human tasks` or `accounting data human tasks`.

   d. Save your changes.

   Example service endpoint, located in `monitorEndpoints.xml`:

```
<tns:Endpoint>
    <tns:id>{com.ibm.wbimonitor}monitorServiceRootId</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorServiceRootId</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/rest/</tns:url>
    <tns:description>Location of backing services for Monitor widgets
</tns:description>
  </tns:Endpoint>
```

3. In the endpoints file, add a widget endpoint for each widget instance.
   a. Edit the endpoints file that you created in step 2. Add an additional widget endpoint starting with `<tns:Endpoint>` and with a unique ID (`<tns:id>`). The type (`<tns:type>`) must have the same value as the ID (`<tns:id>`). The URL for the new endpoint (`<tns:url>`) should be the same as the context root you deployed in step 1., but with beginning and end directory indications, for example, `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`. The widget endpoint you add should contain the same version and can optionally contain all the locales as the original endpoint. You can change the name and description.
   b. When adding endpoints, pay attention to the following information:
      - `<tns:id>`: The ID can be any string but must be unique for all registered endpoints. Ensure that this ID is unique when you are adding additional endpoints.
      - `<tns:type>`: The type must have the same value as `<tns:id>`.
      - `<tns:url>`: For the widget endpoint, make sure the URL is same as the context root you deployed, but with beginning and end directory indications, for example, `<tns:url>/BSpaceWidgetsWPS2/</tns:url>`.
      - `<tns:description>`: Type a meaningful description that further details the nature of the data set that this endpoint is working on. It could either be based on the cluster that is working on the data set or the nature of the data set, for example, `insurance claim human tasks` or `accounting data human tasks`.
   c. Save your changes.

   Example widget endpoint, located in `monitorEndpoints.xml`:

```
<tns:Endpoint>
<tns:id>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:id>
    <tns:type>{com.ibm.wbimonitor}monitorWidgetRootId2</tns:type>
    <tns:version>1.0.0.0</tns:version>
    <tns:url>/newMonitorWidgetContextRoot/</tns:url>
    <tns:description>Location for Monitor widgets</tns:description>
  </tns:Endpoint>
```

4. Create a widget catalog file to add new widget definitions.
   a. Locate the widget catalog file in the *install_root*\BusinessSpace\ registryData\catalogs directory. Copy the catalog template file. For the new file name, use the following standard: `catalog_widget.xml` (with no spaces in the file name), where *widget* is the same as the id value of the `<catalog>` element in the file. Remove all the `<category>` elements that you do not intend to change. For the category that you are working with, remove all the `<entry>` elements that you do not intend to change.
   b. Add an `<entry>` with a unique ID, for example, `id="{com.ibm.bspace.widget}widget_id` and a unique name, for example, `unique-name="{com.ibm.bspace.widget}widget_name`. You can keep all the other definitions.
   c. Change the title and description to make the new widget available as a distinct widget in Business Space that outlines the nature of the new endpoint. For example, you could name your widget `My team's insurance task list` in the `<title>`. The title should help the business users choose the right widget. The description should help the business users understand the nature of the data and the functionality of the widget that they are selecting.
   d. Edit the new widget catalog XML file to reference the new widget endpoint: Change the definition to match the `<tns:id>` of the widget endpoint you added in step 3.a.

For example, change it to: **...**

`<definition>endpoint://`**`{com.ibm.wbimonitor}monitorWidgetRootId2`**`/com/`
`ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>`

...

e. In the `<metadata>` of the catalog file, make sure the `endpoint://` matches the type and the ID in the endpoint file (`<tns:type>` and `<tns:id>`).

f. In the `<metadata>` of the catalog file, make sure the `"refVersion" :` matches the version in the endpoint file (`<tns:version>`).

g. Save your changes.

Example widget catalog file:

```
<entry id="{com.ibm.wbimonitor}instances"
unique-name="{com.ibm.wbimonitor}instances">
        <title>
            <!-- END NON-TRANSLATABLE -->
            <nls-string xml:lang="en">Instances</nls-string>
            <!-- START NON-TRANSLATABLE -->
        </title>
        <description>
            <!-- END NON-TRANSLATABLE -->
            <nls-string xml:lang="en">Instances</nls-string>
            <!-- START NON-TRANSLATABLE -->
        </description>
    <shortDescription>
                <!-- END NON-TRANSLATABLE -->
           <nls-string xml:lang="en">This widget displays a dashboard with
the available monitoring context in either individual instances or user-
defined groups of context instances.</nls-string>
                <!-- START NON-TRANSLATABLE -->
        </shortDescription>
        <definition>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId
/com/ibm/wbimonitor/common/iWidgets/instances_iWidget.xml</definition>
        <content>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
thumb_instances.gif</content>
        <preview>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
prev_instances.gif</preview>
    <previewThumbnail>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/
img/prev_instances.gif</previewThumbnail>
    <help>endpoint://{com.ibm.bspace}bspaceWidgetHelpRootId/topic/
com.ibm.bspace.help.widg.mon.doc/dash/help_instance_whatis.html</help>
        <icon>endpoint://{com.ibm.wbimonitor}monitorWidgetRootId/img/
icon_instances.gif</icon>
    <metadata name="com.ibm.mashups.builder.autoWiringEnabled">true
</metadata>
        <metadata name="com.ibm.bspace.version">7.0.0.0</metadata>
        <metadata name="com.ibm.bspace.owner">International Business
Machines Corp.</metadata>
        <metadata name="com.ibm.bspace.serviceEndpointRefs">
[{"name":"serviceUrlRoot", "required":"true",
"refId":"endpoint://{com.ibm.wbimonitor}monitorServiceRootId",
"refVersion":"1.0.0.0"}]</metadata>
        </entry>
```

5. Place the new endpoint file and the new catalog file in a compressed file, and run the updateBusinessSpaceWidgets command, using the **-widgets** parameter to specify the compressed file location..

What to do next

- After running the updateBusinessSpaceWidgets command, you must perform manual steps to update Business Space templates and spaces. For more information, see Updating Business Space templates and spaces after installing or updating widgets.

- If Business Space is running on a different cell than where the REST services are running, you must manually edit the endpoints files.

- If you have enabled security for your environment, you must make sure that it is set up properly to work with Business Space.

Configuring widgets for multiple products

You can configure or add Business Space widgets for one BPM product on a Business Space that has already been configured with a different BPM product by using the installBusinessSpaceWidgets command.

Before you begin

Before you complete this task, you must have completed the following tasks:
- Completed all steps to install and configure a BPM product, and configured Business Space.
- Completed all steps to install and configure the additional BPM product.

About this task

You can install more than one BPM product that works with Business Space and configure the widgets for both products after you install the second product. However, if you install a second BPM product after you have already configured Business Space with widgets for the first product, you must use the installBusinessSpaceWidgets command to add and configure the second product widgets to work with the same Business Space.

In a stand-alone augmentation, widgets are installed automatically. For example, widgets are installed if you create a WebSphere Process Server stand-alone profile, configure the server for Business Space, install WebSphere Business Monitor, and augment the already-configured server to WebSphere Business Monitor. But for a network deployment environment, when you augment a deployment manager to another product, no additional widgets are installed and configured.

Procedure

1. Make sure the deployment manager profile is up and running, and on that profile, open a command window.

   The wsadmin command can be found at the `profiles/`*`profile_name`*`/bin` directory.
2. At the command prompt, type the wsadmin command to start the wsadmin environment.
3. Use the installBusinessSpaceWidgets command to install, deploy, and register designated widgets located in the *`install_root`*`/BusinessSpace/widgets` directory.

Example

The following example uses Jython to run the installBusinessSpaceWidgets to install widgets for IBM WebSphere Business Monitor to work with the Business Space environment that has been previously configured for IBM WebSphere Process Server.

```
AdminTask.installBusinessSpaceWidgets('[-nodeName node_name
 -serverName server_name -widgets
 install_root\BusinessSpace\widgets\WBM\Widgets_WBMonitor.zip]')
```

The following example uses Jacl:

```
$AdminTask installBusinessSpaceWidgets {-nodeName node_name
 -serverName server_name -widgets
 install_root\BusinessSpace\widgets\WBM\Widgets_WBMonitor.zip}
```

What to do next

To enable Business Space for your runtime environment, you must perform the following steps after configuring the widgets.

- After running the installBusinessSpaceWidgets command or the updateBusinessSpaceWidgets command, perform manual steps to update Business Space templates and spaces. For more information, see Updating Business Space templates and spaces after installing or updating widgets.
- Configure REST services. For more information, see Configuring REST services.
- Register REST endpoints. For more information, see "Configuring Business Space and registering REST endpoints on the administrative console."
- Verify security is set up properly to work with Business Space and the widgets your team is using. For more information, see Setting up security for Business Space.

Setting up specific widgets to work in Business Space

Some of the widgets that come with your product require additional configuration steps before you can use them in Business Space.

About this task

Your business process management product includes several widgets, and some require additional configuration to communicate with your solution from Business Space.

Configuring the service monitor

If you are creating a new server and you want to use the Service Monitor widget (available in Business Space) to measure the response time and request throughput for services exposed or invoked by an SCA module, configure and enable service monitoring in the administrative console.

Before you begin

Required security role for this task: If administrative security is enabled, you must be logged in with an administrative role to perform this task.

About this task

The service monitor has a client/server architecture.

- Service monitor agent: Measures the throughput and response time for operations and sends the measurement data to the service monitor server
- Service monitor server: Gathers and aggregates response time and throughput measurements from all running service monitor agents, and then calculates and stores the statistics.

In a deployment environment, the server runs on a support cluster, while the agent runs in the application cluster on the server where you deployed your module. In a stand-alone server environment, the server and agent both run on the stand-alone server.

Important: If you are using an external HTTP server to access Business space, make sure to configure the HTTP server to allow encoded slashes. Refer to the HTTP server documentation for details.

Procedure

1. Log into the administrative console with administrator privileges.
2. Configure the service monitor server.
   a. From within the console, click **Servers** → **Server Types** → **WebSphere application servers** → *servername* → **Service Monitor**.
   b. On the Service Monitor page, click **Enable service monitor**.
   c. Examine the default values for the service monitor buffer size and the query size limit and, if necessary, revise them.
   d. Specify the service monitoring targets. These are the service monitor agents you want to gather data from.

Table 187. Monitoring

Targets to monitor	Steps to perform
Monitor all running service monitor agents	Ensure the **All enabled service monitor agents** option is checked.
Monitor a specific subset of running service monitor agents	1. Clear the **All enabled service monitor agents** option. A collection table appears; if this is a new configuration, the table is empty. 2. Click **Add**. The Browse Deployment Targets page opens. 3. From the collection table on the Browse Deployment Targets page, select the deployment target whose agent you want to monitor. 4. Click **OK** to return to the Service Monitor Server page. 5. Repeat Step 2 through Step 4 until you have added all the agents you want to monitor.

   e. From the Service Monitor Server page, click **OK**. The configuration is saved and takes effect immediately.
3. Configure the service monitor agent.
   a. From within the console, click **Servers** → **Server Types** → **WebSphere application servers** → *servername* → **Service Monitor Agent**.
   b. On the Service Monitor Agent page, click **Enable service monitor agent**.
   c. Examine the default values for the agent configuration and, if necessary, revise them.
   d. Click **OK**.

Enabling forms for running Human Task Management widgets in Business Space

If you are working with WebSphere Process Server, you must take additional steps to enable forms for working with Human Task Management widgets in Business Space.

About this task

Topic scope: This topic applies to the following products:
- WebSphere Business Compass
- WebSphere Business Monitor

- WebSphere Process Server
- WebSphere Business Services Fabric

If you have installed Business Space on a different server instance than Business Process Choreographer, you must take additional steps to make forms deployed in separate enterprise applications available to the Human Task Management widgets. This includes HTML-Dojo forms that are generated in WebSphere Integration Developer and IBM Lotus Forms.

Depending on whether both Business Space and WebSphere Process Server are configured on deployment targets in the same WebSphere Network Deployment cell or in different cells, complete one of the following steps:

Procedure

1. For a setup in a single cell: When deploying an enterprise application that contains a process or a human task and forms, you must map the Web modules that contain the HTML files or Lotus form definitions for the forms to the same deployment target that Business Space is configured on.

2. For a setup in a cross-cell environment: Deploy the Web module containing the HTML files or Lotus form definitions for the forms on the deployment target that hosts Business Space in the remote cell. When deploying the Web module, you must specify the context root as defined for the forms in the Human Task Editor in WebSphere Integration Developer. Start the new application on the Business Space server or cluster.

What to do next

If you are using Lotus Webform Server to work with the Human Task Management widgets, you must configure Lotus Webform Server for Business Space.

Configuring Lotus Webform Server for Human Task Management widgets in Business Space:

If you are working with WebSphere Process Server Human Task Management widgets, and you want to use Lotus Webform Server to work with forms during runtime, you must configure Business Space to use Lotus Webform Server.

Before you begin

Before you can use Lotus Webform Server with the Human Task Management widgets in Business Space, you must install Lotus Webform Server 3.5.1 with fix pack 1 or later.

Webform Server can only run on a machine with 32-bit architecture.

When you install Webform Server, make sure to select both **Webform Server - Application Server** and **Webform Server - Translator Server** on the Server components page on the installation tool. On the Optional Deployment settings page, make sure to select **Deploy Webform Server - Translator Server to WebSphere Application Server**. Do not select **Deploy API to WebSphere Application Server or WebSphere Process Server**.

Note: If you are using a Derby database, you must install Lotus Webform Server in a separate profile. It cannot use the same profile as Business Space and WebSphere Process Server.

About this task

Topic scope: This topic applies to the following products:
- WebSphere Business Compass
- WebSphere Business Monitor
- WebSphere Process Server
- WebSphere Business Services Fabric

Depending on your environment, perform one of the following three steps.

Procedure
1. If you have a single-server environment and Lotus Webform Server is already installed on the same system as WebSphere Process Server, configure Lotus Webform Server for Business Space by using the Profile Management Tool. Otherwise, go to step 2.
   a. Start the Profile Management Tool, and create a stand-alone server profile.
   b. On the Profile Creation Options page, select the **Advanced** option.
   c. On the Business Space Configuration page, select the **Configure Lotus Webform Server** check box and enter the Webform Server translator and installation root. For more information, see Creating Advanced stand-alone server profiles.
2. If Lotus Webform Server is installed on the same system where WebSphere Process Server is installed (and you did not configure Lotus Webform Server in the Profile Management Tool), perform the following steps. Otherwise, go to step 3.
   a. For your profile, open a command window. The wsadmin command can be found at the `profiles\`*`profile_name`*`\bin` directory. For a clustered environment, run the command from the *`deployment_manager_profile_root`*`\bin` directory. For a stand-alone server environment, run the command from the *`profile_root`*`\bin` directory.
   b. At the command prompt, type the wsadmin command to start the wsadmin environment. For example, on Windows platforms, type `wsadmin.bat -conntype NONE`.
   c. On the same machine where Webform Server is located, run the configureWebformServer command, designating the local host and location.

   For example, run the following command using Jython:

   ```
   AdminTask.configureLotusWebformServer(['-nodeName', node_name,
   '-serverName', server_name, '-translatorHTTPLocation',
   'http://localhost:8085/translator', '-serverInstallRoot',
   'C:/IBM/LotusWebForms/3.5/WebFormServer'])
   AdminConfig.save()
   ```

   Or, run the following command using Jacl:

   ```
   $AdminTask configureLotusWebformServer {-nodeName node_name -serverName
   server_name -translatorHTTPLocation http://localhost:8085/translator
   -serverInstallRoot C:/IBM/LotusWebForms/3.5/WebFormServer}
   $AdminConfig save
   ```

3. If Lotus Webform Server is installed on a different system than where WebSphere Process Server is installed, complete the following steps.

   a. Copy the `BSpaceWebformsEnabler.ear` from the *profile root*`/installableApps/BusinessSpace` directory to the system that has Webform Server installed. Deploy this ear on the remote application server.

   b. On the local Business Space profile, in the `bspaceWFSEndpoints.xml` file, set the endpoint `{com.ibm.bspace}bspaceWebformsProxyRootId` to reference the fully qualified location of the `BSpaceWebformsEnabler.ear`. For more information about editing endpoints files, see Enabling Business Space widgets manually for cross-cell environments.

   c. On the Webform Server system, open the administrative console on the profile where you configured the Lotus Webform Server.

   d. Set the following variables by clicking **Environment** → **WebSphere Variables**, then selecting the node that contains the server that you are using, and then clicking **New** for setting each new variable.

      • Set the Webform Server Install Directory variable by creating a variable with the name LFS_DIR and value of the Webform Server Install, for example, `c:\Program Files\Lotus Webform Server\3.5\WebformServer`.

      • Set the LFS_API_DIR variable by creating a variable with the name `LFS_API_DIR` and value `$(LFS_DIR)\Translator\API`.

      • Set the LFS_API_LIB_DIR variable by creating a variable with the name `LFS_API_LIB_DIR` and value `$(LFS_API_DIR)\76\java\classes`.

      • Set the LFS_DEP_DIR variable by creating a variable with the name `LFS_DEP_DIR` and value `$(LFS_DIR)\redist`.

      • `UNIX` `Linux` For AIX, Linux, and Solaris operating systems, set the UWIJAVA variable by creating a variable with the name `UWIJAVA` and the value of the JVM library. This value is dependant on your operating system:

        – On AIX: *process_server_install_root*/java/jre/lib/ppc/j9vm/libjvm.a
        – On Linux: *process_server_install_root*/java/jre/lib/i386/libjava.so
        – On Solaris: *process_server_install_root*/java/jre/lib/sparc/libjava.so

   e. Set the Java Process Definition.

      • Click **Servers** → **Server Types** → **WebSphere application servers** → *server_name* → **Java and Process Management** → **Process Definition** → **Environment Entries**.

      • `Windows` On Windows: Add a PATH property and point it to the API directories that contain .dll files, for example: `${LFS_API_DIR};${LFS_API_DIR}/76/system;`

      • `UNIX` On AIX: Add a LIBPATH property and point it to the API directories that contain .so files, for example: `${LFS_API_DIR}:${LFS_API_DIR}/76/system;`

      • `UNIX` `Linux` On Solaris and Linux: Add a LD_LIBRARY_PATH property and point it to the API directories that contain .so files, for example: `${LFS_API_DIR}:${LFS_API_DIR}/76/system;`

      Note: If the LD_LIBRARY_PATH, LIBPATH, or PATH properties have already been created, add the API directory paths to the existing properties. Remember to use the correct separator; Windows uses a semicolon, but AIX, Linux, and Solaris platforms use a colon.

- Add a `PUREEDGE_INI` property and value: `${LFS_DIR}\Translator\`
  `PureEdgeAPI.ini`.

f. Set the LFS_API_LIB and LFS_DEP_LIB shared libraries.
  - Click **Environment** → **Shared Libraries**.
  - Set the scope by selecting the node that contains the server that you are using. The scope must be the same scope as the environment variable settings.
  - Click **New**.
  - Create an entry with name: "LFS_API_LIB" and classpath (one per line):
    - ${LFS_API_LIB_DIR}/pe_api.jar
    - ${LFS_API_LIB_DIR}/pe_api_native.jar
    - ${LFS_API_LIB_DIR}/uwi_api.jar
    - ${LFS_API_LIB_DIR}/uwi_api_native.jar
    - ${LFS_API_LIB_DIR}/commons-codec.jar
    - ${LFS_API_LIB_DIR}/xmlsec-1.4.1.jar
  - Click **OK**.
  - Click **New**.
  - Create an entry with name: "LFS_DEP_LIB" and classpath (one per line):
    - ${LFS_DEP_DIR}/commons-codec-1.3.jar
    - ${LFS_DEP_DIR}/commons-httpclient-3.0.jar
    - ${LFS_DEP_DIR}/ehcache-1.2.2.jar
    - ${LFS_DEP_DIR}/log4j-1.2.8.jar
    - ${LFS_DEP_DIR}/ws_common.jar
    - ${LFS_DEP_DIR}/ws_framework.jar
    - ${LFS_DEP_DIR}/ws_resourcestore.jar
    - ${LFS_DEP_DIR}/ws_resourcebundle.jar
  - Click **OK**.

g. Set the server class loader.
  - Click **Servers** → **Server Types** → **WebSphere application servers** → *server_name* → **Java and Process Management** → **Classloader**.
  - If a class loader for your application server does not exist, you must create it. Click **New** and select the parent last option.
  - Select the class loader for your application server and click **Shared Library References**.
  - Click **Add**.
  - From the Library Name list, select LFS_API_LIB.
  - Repeat for library: LFS_DEP_LIB
  - Click **OK**.

h. Configure the Webform Translator location.
  - Ensure that the BSpaceWebformsEnabler EAR has been deployed
  - Click **Applications** → **Application types** → **WebSphere enterprise applications** → **BSpaceWebformsEnabler** → **Initialize parameters for servlets**.
  - Set the value for the `translatorLocation` to the http address of the Webform Server Translator. If the Translator has been configured to run on the same machine as the `BSpaceWebFormsEnabler`, Then leave the default value of: `http://localhost:8085/translator`

i. Save all changes to the master configuration, and restart the server.

Enabling images in Human Task Management widgets

If you are setting up Business Space to include Human Task Management widgets, you can create an endpoints file to use images of team members in those widgets. All widgets that are configured to display a user ID and allow grouping by this user ID can be enabled to display images.

Before you begin

Topic scope: This topic applies to the following products:
- WebSphere Business Compass
- WebSphere Business Monitor
- WebSphere Process Server
- WebSphere Business Services Fabric

About this task

By default, Business Space is configured with no image server identified for Human Task Management widgets, but if you want your business users to see images of their team members, you can enable image retrieval in a new widget endpoint file.

Procedure

1. Create a new file in *install_root*\BusinessSpace\registryData\ For example, name it `imageEndpoint.xml`.

2. Copy in the following template.

```
<?xml version="1.0" encoding="UTF-8"?>
<tns:BusinessSpaceRegistry xmlns:tns="http://com.ibm.bspace/
BusinessSpaceRegistry" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://com.ibm.bspace/BusinessSpaceRegistry
 BusinessSpaceRegistry.xsd ">
<tns:Endpoint>
<tns:id>{com.ibm.bspace.htm}bspaceUserImageServiceRootId</tns:id>
<tns:type>{com.ibm.bspace.htm}bspaceUserImageServiceRootId</tns:type>
<tns:version>1.0.0.0</tns:version>
<tns:url>URL</tns:url>
<tns:description>Location of user image services</tns:description>
</tns:Endpoint>
</tns:BusinessSpaceRegistry>
```

3. Update the URL to reference the appropriate image server servlet that you are using for user images.

   The image service endpoint is a reference to a URL prefix where the widgets can find images by concatenating the following information:
   - The resolved image service endpoint string.
   - The unique identifier Virtual Member Manager (VMM) attribute for each user.
   - The .jpg file extension.

   For example, if the endpoint URL is `http://myserver:9080/UserImageWeb/UserImageServlet/` and the unique identifier for a user is `id123456`, the widgets retrieve that user's image at the following link: `http://myserver:9080/UserImageWeb/UserImageServlet/id123456.jpg`.

4. Run the updateBusinessSpaceWidgets command.

   a. For your profile, open a command window.

      The wsadmin command can be found at the `profiles/`*profile_name*`/bin` directory.

b. Use the updateBusinessSpaceWidgets command to install, deploy, and register the designated widgets.

Setting up security for Business Space

If you are using Business Space powered by WebSphere with your environment, you must consider security options for how your team will work with artifacts in Business Space. If you want to turn on security for Business Space, set up application security and designate a user repository. To define Business Space administrators, assign a superuser role.

About this task

For best results, enable security before you configure Business Space. On the administrative console Global security administration page, you enable both administrative security and application security. You also designate a user account repository.

Considerations for using a user account registry with Business Space:

- Based on the type of LDAP configuration that you are using, your settings can impact your ability to access Business Space correctly. Make sure that the user filters, the group filters, and mapping settings are configured properly. For more information, see Configuring Lightweight Directory Access Protocol search filters in the WebSphere Application Server documentation.
- Based on the type of federated repository configuration that you are using, your settings can affect your ability to access Business Space correctly. Make sure that the realms are configured properly. For more information, see Managing the realm in a federated repository configuration in the WebSphere Application Server documentation.
- The LDAP security is set up by default to use the login property `uid` (user ID) for searching in Business Space. If your LDAP security is changed to use another unique LDAP field, such as `mail` (e-mail address) for the login property, then you must modify the userIdKey property in the `ConfigServices.properties` file in order for searching to work in Business Space. The `ConfigServices.properties` file is located at *profile_root*\BusinessSpace\ *node_name**server_name*\mm.runtime.prof\config\ConfigService.properties for a stand-alone server or *deployment_manager_profile_root*\BusinessSpace\ *cluster_name*\mm.runtime.prof\config\ConfigService.properties for a cluster. Change the userIdKey attribute from `uid` to match the login property for your LDAP security, for example, `mail`. Then run the updatePropertyConfig command using the wsadmin scripting client, designating the following parameters: **-serverName** and **-nodeName** for a stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the value of the path for the `ConfigServices.properties` file, and **-prefix** with the value `Mashups_`.
- If you are using a Microsoft SQL Server database and the **Standalone LDAP** registry, make sure that the user distinguished name (user DN) does not exceed 131 characters. If any of the user DN entries exceed 131 characters, you must designate the **Federated repositories** option for the user account repository. When switching between federated repositories and other registries, all the existing spaces, pages are no longer accessible in Business Space and must be created again.
- If you are using **Federated repositories**, you have additional capabilities in your widgets and framework, such as enhanced search capabilities. When searching for users to share spaces and pages, the search scope includes e-mail, a full user name, and user ID.

If you are using IBM Tivoli Access Manager WebSEAL and want to use it with your Business Space environment, you must complete additional configuration steps. Configure Tivoli Access Manager security with an external Java Authorization Contract for Containers (JACC) provider, configure WebSEAL with Tivoli Access Manager, configure WebSEAL with your product application server, and configure host junctions for your environment.

To set up which users in the Business Space environment will be administrators, you run a script to assign the Business Space superuser role.

Setting application security for Business Space

To turn on security for Business Space you must enable both application security and administrative security.

Before you begin

Before you complete this task, you must have completed the following tasks:

- Checked that your user ID is registered in the user registry for your product.

If you expect to use a secured environment, make sure to enable security before you configure Business Space. If you want to enable or remove security after you have configured Business Space, you must modify both the `MashupAdminForOOBSpace` property and the `noSecurityAdminInternalUserOnly` property in the `ConfigServices.properties` file to set the correct user ID as the valid administrator ID. The `ConfigServices.properties` file is located at *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ `ConfigService.properties` for a stand-alone server or *deployment_manager_profile_root*\BusinessSpace*cluster_name*\mm.runtime.prof\ config\ConfigService.properties for a cluster. Copy the modified file into an empty folder on your system. Then run the updatePropertyConfig command using the wsadmin scripting client, designating the following parameters:

- **-serverName** and **-nodeName** for a stand-alone server or **-clusterName** for a cluster
- **-propertyFileName** with the value of the path for the `ConfigServices.properties` file
- **-prefix** with the value `Mashups_`

About this task

Business Space is preconfigured to ensure authentication and authorization of access. Users are prompted to authenticate when accessing Business Space URLs. Unauthenticated users are redirected to a login page. Business Space can be accessed by either HTTP or HTTPS, except for the login page, which always redirects to HTTPS. Therefore if using a Web server such as the IBM HTTP Server, you must configure it to support HTTPS.

Authorization to spaces and page content in Business Space is handled internally to Business Space as part of managing spaces.

To enable authenticated access to Business Space, you must have a user registry configured and application security enabled.

Procedure

1. For complete instructions on security, see the security documentation for your product.

2. For the Business Space application, on the Global security administrative console page, select both **Enable administrative security** and **Enable application security**.

3. On the same administrative console page, under **User account repository**, designate either **Federated repositories**, **Local Operating System**, **Standalone LDAP registry**, or **Standalone custom registry**. Review the considerations for selecting a user registry in Setting up security for Business Space.

4. If Business Space is remote from where your product is running, and if the node where Business Space is running and the node where your product is running are not in the same cell, you must complete manual steps to make sure that single-sign-on (SSO) is enabled. For example, if you are using more than one product (WebSphere Business Compass, WebSphere Business Monitor, WebSphere Enterprise Service Bus, or WebSphere Process Server), the servers are on different nodes, and you want them all to be able to work with the Business Space server, you must manually configure SSO. To enable SSO, complete the following steps:

   a. On the administrative console for each server, open the Global security page by clicking **Security ▸ Global security**. Expand **Web and SIP security** and click **single sign-on (SSO)** to make sure that the **Enabled** check box is selected.

   b. Make sure that all the nodes use the same **User account repository** information (see step 3).

   c. On the administrative console for the first node, open the Global security page. Under Authentication, click **LTPA**.

   d. Under **Cross-cell single sign on**, type a password for the key file and a fully qualified key file name, which is a location and file name where you want to export the key file. The fully qualified key file name is the absolute path on the system where your server is running.

   e. Click **Export keys**. The key file is saved on the system where the server is running.

   f. If the two nodes are not on the same system, copy the key file physically to the other systems.

   g. Import the key file on every other node using the same key file: Log on to the administrative console for the other nodes, and go to the Global security > LTPA page. Under **Cross-cell single sign on**, type the password for the key file and the fully qualified key file name (use the same password for the exported key file that you copied over), and click **Import keys**.

   h. Restart the server after importing keys on each system.

5. If you are using HTTPS in the endpoints file, the endpoint location is on a different node than Business Space, and the Secure Sockets Layer (SSL) certificate is a self-signed SSL certificate, you must import it.

   a. Log on to the administrative console for the server that contains Business Space and import the SSL certificate that is used by the remote node where product is running.

      1) Under Security, click **SSL certificate and key management**.

      2) On the SSL certificate and key management page, under Related items, click **Key stores and certificates**.

      3) On the Key stores and certificates page, click **NodeDefaultTrustStore** to modify that truststore type.

      4) On the NodeDefaultTrustStore page, under Additional Properties, click **Signer certificates**.

5) On the Signer certificates page for the **NodeDefaultTrustStore**, click the **Retrieve from port** button.

6) On Retrieve from port page, under General Properties, type the host, port, and alias for where your product is running. Click **Retrieve signer information** button and then click **OK**.

7) Restart both servers.

b. Log on to the administrative console for the product node and import the SSL certificate that is used by the node where Business Space is running.

1) Repeat steps a. i.-v.

2) On the Retrieve from port page, under General Properties, type the host and port for where Business Space is running. Click the **Retrieve signer information** button and then click **OK**.

3) Restart both servers.

For more information about SSO and SSL, see the WebSphere Application Server information center.

What to do next

- After the administrative security and application security are turned on, you receive a prompt for a user ID and password when you log on to Business Space. You must use a valid user ID and password from the selected user registry in order to log on. After you turn on administrative security, whenever you return to the administrative console, you must log on with the user ID that has administrative authority.

- If you want to restrict logging in to Business Space to a subset of users and groups, you can change the mapping of the Business Space J2EE role. You must update the user/group mapping for two enterprise applications: **BSpaceEAR_*node_server*** and **mm.was_*node_server***. Click **Applications** → **Application Types** → **WebSphere enterprise applications** and select the two applications. In the right panel, under Detail Properties, select **Security role to user/group mapping**. Remap the **businessspaceusers** and **Allauthenticated** roles from the two applications by first removing the special subject. Click **Map Special Subjects** and select **None**. Then click **Map Users** or **Map Groups** and assign each role to your selected users or groups. Note that changing the J2EE role mapping does not affect the user/group search function in Business Space.

- To set authorization to pages and spaces in Business Space, you can manage authorization when you create Business Space pages and spaces.

- Monitor Process Server / ESB To set up security for the data in the widgets based on users and groups, you must modify the mapping of users to the REST services gateway application. Select the REST services gateway application, and in the right panel, under Detail Properties, select **Security role to user/group mapping**. For the RestServicesUser role, you can add users and groups to it to control access to the data in all the REST services widgets.

- Process Server / ESB If you want to restrict access to data in the widgets based on user group roles, consider changing the users assigned to the administrative group roles. You can view the Roles list to see who is assigned to these roles by opening the administrative console, clicking **Security** → **Secure administration, applications, and infrastructure** → **Administrative Group Roles**, and selecting a group.

  You might want to consider changing the users assigned to administrative group roles for widgets such as Business Rules and Business Variables.

For example, for the System Health widget, the following administrative roles all have monitoring permissions, all allow access to the administrative console, and therefore allow users assigned to those roles to access data in the System Health widget:

– **Monitor**
– **Configurator**
– **Operator**
– **Administrator**
– **Adminsecuritymanager**
– **Deployer**
– **iscadmins**

Users who are mapped to those administrative group roles have access to the data in the System Health widget. Users who are not mapped to those roles cannot access the data in the System Health widget.

• Finally, some widgets have an additional layer of role-based access for their artifacts created by business users. For WebSphere Process Server administration widgets, the Security Roles widget allows you to assign users and groups to system roles or module roles that determine the level of access that members have for timetables in the Business Calendars widget. For WebSphere Business Compass, the Review Access Control widget manages permissions for users who can review and comment on reviews. For more information, see the online help for your widgets.

Note:

If you find the following errors in the `SystemOut.log` file, you might have extra attributes in your user registry that cannot be processed:

```
00000046 SystemErr R Caused by: com.ibm.websphere.wim.exception.WIMSystemException: CWWIM1013E
    The value of the property secretary is not valid for entity uid=xxx,c=us,ou=yyy,o=ibm.com.
00000046 SystemErr R at com.ibm.ws.wim.adapter.ldap.LdapAdapter.setPropertyValue(LdapAdapter.java:3338)
```

Set the following attributes in the `ConfigServices.properties` file to bypass those attributes:

```
com.ibm.mashups.user.userProfile = LIMITED
com.ibm.mashups.user.groupProfile = LIMITED
```

The `ConfigServices.properties` file is located at *profile_root*\BusinessSpace\ *node_name**server_name*\mm.runtime.prof\config\ConfigService.properties for a stand-alone server or *deployment_manager_profile_root*\BusinessSpace\ *cluster_name*\mm.runtime.prof\config\ConfigService.properties for a cluster. After modifying the `ConfigServices.properties` file, run the updatePropertyConfig command using the wsadmin scripting client, designating the following parameters: **-serverName** and **-nodeName** for a stand-alone server or **-clusterName** for a cluster, **-propertyFileName** with the value of the path for the `ConfigServices.properties` file, and **-prefix** with the value `Mashups_`.

Note:

If you have Java 2 security enabled in a cluster, consider tightening the entry in the server policy applied to the Business Space help location.

The Business Space help location policy is:

```
grant codeBase      "file:${was.install.root}/profiles/profile_name/temp/
node_name/-" {

    permission java.security.AllPermission;

};
```

Tighten the policy by changing it to:

```
grant codeBase      "file:${was.install.root}/profiles/profile_name/temp/
node_name/server_name/BusinessSpaceHelpEAR_node_name_server_name/
BusinessSpaceHelp.war/-" {

    permission java.security.AllPermission;

 };
```

Configuring Tivoli Access Manager WebSEAL to work with Business Space

If you have Tivoli Access Manager WebSEAL and you want to use it with Business Space, you must complete several additional configuration steps.

About this task

If you want to use Tivoli Access Manager WebSEAL with Business Space, you must configure Tivoli Access Manager security with an external Java Authorization Contract for Containers (JACC) provider, configure WebSEAL with Tivoli Access Manager, configure WebSEAL with your product application server, and configure host junctions for your environment.

Procedure

1. Configure Tivoli Access Manager with JACC.
   a. Complete one of the following steps, depending on whether you want to use the administrative console or the wsadmin commands.
      • If you want to use the administrative console to configure Tivoli Access Manager with JACC, complete the following steps:
        1) Enable Global Security.
           a) Select **Security → Global Security**.
           b) Enable **Administrative security**, **Application security**, and **Java 2 security** with the LDAP server with which Tivoli Access Manager is configured.
           c) Select **Global Security → LDAP**, enter the following information, and then click **OK**.

Name	Description
Server user Id	Enter the same user ID that you entered for the administrator DN on Tivoli Access Manager settings. Example: user1
Server user password	puser1
Host	LDAP configured with Tivoli Access Manager
Port	Example: 389
Base DN	Example: o=ibm, c=us

Name	Description
`Bind DN`	Example: `cn=SecurityMaster,secAuthority=Default`
`Bind pwd`	password for SecurityMaster user

      d) Save the configuration, and restart the server.

   2) Enable external authorization with Tivoli Access Manager and JACC.

      a) Select **Security** → **Global Security** → **External authorization providers**.

      b) In the **Authorization provider** list, select **External JACC provider**, and then click **Configure**. The default properties for Tivoli Access Manager are correct. For default values, do not change.

      c) Under **Additional Properties**, select **Tivoli Access Manager properties**. Select **Enable embedded Tivoli Access Manager**, enter the following information, and then click **OK**.

Name	Value
Client listening port set	The default setting is 8900 - 8999. Change it only if you want to use different ports.
Policy server (name:port)	Specify your *policyserver:port*. Example: `windomain3.rtp.raleigh.ibm.com:7135`
Authorization servers and priority (name:port:priority)	Specify your *authorizationserver:port:priority*. Example: `windomain3.rtp.raleigh.ibm.com:7136:1`
Administrator user name	Leave the user name as **sec_master (default)**, unless you use a different admin name on the Tivoli Access Manager server.
Administrator user password	`domino123`
User registry distinguished name suffix	Type the name that you want to use for your application server. Example: `o=ibm,c=us`
Security domain	Leave the Security domain set to **Default**. Change this setting if you are not using the default domain on the Tivoli Access Manager server. Change this setting if you have multiple domains created on the Tivoli Access Manager server and you want to connect or use a domain other than **Default**.
Administrator user distinguished name	Type the fully qualified name of the user. Example: `cn=user1,o=ibm,c=us` **Note:** This user is the same as the **Server user ID** configured in the LDAP user registry panel.

      The server contacts the Tivoli Access Manager server and creates several properties files under the application server. This process might take a few minutes. If an error occurs, look in `system Out` and correct the problem.

- If you want to use the wsadmin utility to configure Tivoli Access Manager with JACC, complete the following steps. Perform the following procedure once on the deployment manager server. The configuration parameters are forwarded to managed servers, including node agents,

when a synchronization is performed. The managed servers require their own restart for the configuration changes to take effect.

1) Verify that all the managed servers, including node agents, are started.

2) Start the server.

3) Start the command-line utility by running the wsadmin command from the *install_root*/bin directory.

4) At the wsadmin prompt, run the configureTAM command, including the appropriate information from the following table:

Jacl example:

```
$AdminTask configureTAM -interactive
```

Jython example:

```
AdminTask.configureTAM('-interactive')
```
Then type the following information:

Name	Value
node name for your product server	Specify a single node or enter an asterisk (*) to choose all nodes.
Tivoli Access Manager Policy Server	Type the name of the Tivoli Access Manager policy server and the connection port. Use the format, *policy_server:port*. The policy server communication port is set at the time of Tivoli Access Manager configuration. The default port is 7135.
Tivoli Access Manager Authorization Server	Type the name of the Tivoli Access Manager authorization server. Use the format *auth_server:port:priority*. The authorization server communication port is set at the time of Tivoli Access Manager configuration. The default port is 7136. You can specify more than one authorization server by separating the entries with commas. Having more than one authorization server configured is useful for failover and performance. The priority value is the order of authorization server use. For example: `auth_server1:7136:1,auth_server2:7137:2`. A priority of 1 is still required when configuring against a single authorization server.
administrator distinguished name for your product server	Type the full distinguished name of the security administrator ID for your product server. For example: `cn=wasadmin,o=organization,c=country`. For more information, see the related link.
Tivoli Access Manager user registry distinguished name suffix	For example: o=organization, c=country
Tivoli Access Manager administrator user name	Type the Tivoli Access Manager administration user ID, as created at the time of Tivoli Access Manager configuration. This ID is typically sec_master.
Tivoli Access Manager administrator user password	Type the password for the Tivoli Access Manager administrator.

Name	Value
Tivoli Access Manager security domain	Type the name of the Tivoli Access Manager security domain that is used to store users and groups. If a security domain is not already established at the time of Tivoli Access Manager configuration, click **Return** to accept the default.
Embedded Tivoli Access Manager listening port set	The product server listens on a TCP/IP port for authorization database updates from the policy server. Because more than one process can run on a particular node and machine, a list of ports is required for the processes. Specify the ports that are used as listening ports by Tivoli Access Manager clients, separated by a comma. If you specify a range of ports, separate the lower and higher values by a colon. For example, 7999, 9990:9999.
Defer	Set to yes, this option defers the configuration of the management server until the next restart. Set to no, configuration of the management server occurs immediately. Managed servers are configured on their next restart.

5) After you enter all the required information, select **F** to save the configuration properties or **C** to cancel from the configuration process and discard the entered information.

Example with SVTM TAM60 server:

```
wsadmin>$AdminTask configureTAM -interactive
Configure embedded Tivoli Access Manager

This command configures embedded Tivoli Access Manager on the WebSphere
Application Server node or nodes specified.

WebSphere Application Server Node Name (nodeName): *
*Tivoli Access Manager Policy Server (policySvr):
 windomain3.rtp.raleigh.ibm.com:7135
*Tivoli Access Manager Authorization Servers (authSvrs):
 windomain3.rtp.raleigh.ibm.com:7136:1
*WebSphere Application Server administrator's distinguished name (wasAdminDN):
 cn=was61admin,o=ibm,c=us
*Tivoli Access Manager user registry distinguished name suffix (dnSuffix):
o=ibm,c=us
Tivoli Access Manager administrator's user name (adminUid):
 [sec_master]
*Tivoli Access Manager administrator's user password (adminPasswd):
 domino123
Tivoli Access Manager security domain (secDomain): [Default]
Embedded Tivoli Access Manager listening port set (portSet): [9900:9999]
Defer (defer): [no]

Configure embedded Tivoli Access Manager

F (Finish)
C (Cancel)

Select [F, C]: [F] F
WASX7278I: Generated command line: $AdminTask configureTAM {-policySvr
 windomain3.rtp.raleigh.ibm.com:7135 -authSvrs
 windomain3.rtp.raleigh.ibm.com:7136:1 -wasAdminDN cn=wa
```

```
Embedded Tivoli Access Manager configuration action parameters saved successfully.
 Restart all WebSphere Application Server instances running on the target node or
 nodes to
wsadmin>
```

6) In the administrative console, select **Security → Global Security →
   External authorization providers**. Then select **External authorization
   using a JACC provider**, and click **OK**.

7) Go to the main security screen and click **OK**. Save and synchronize
   your changes.

8) Restart all processes in your cell.

b. If you installed applications before you enabled Tivoli Access Manager (for
   example, you enabled LDAP security and installed some secured
   applications and mapped users and groups to security roles), propagate the
   security roles mapping information from the deployment descriptors to the
   Tivoli Access Manager policy server. Perform one of the following steps,
   depending on whether you want to use the administrative console, or the
   wsadmin commands.

   • If you want to use the propagatePolicyToJACCProvider wsadmin
     command, see Propagating security policy of installed applications to a
     JACC provider using wsadmin scripting.

   • If you want to use the administrative console, see Propagating security
     policies and roles for previously deployed applications.

2. Configure WebSEAL with Tivoli Access Manager.

   a. Ensure that WebSEAL is installed and configured properly.

   b. Create the junction between WebSEAL and your product application server
      using the **-c iv_creds** option for TAI++ and **-c iv_user** for TAI. Enter either
      of the following commands as one line, using the variables that are
      appropriate for your environment:

      For TAI++

      ```
      server task webseald-server create -t tcp -b supply -c iv_creds
      -h host_name -p websphere_app_port_number junction_name
      ```

   c. To create a trusted user account in Tivoli Access Manager, which can be
      used for configuring TAI, issue the following commands:

      ```
      pdadmin -a sec_master -p domino123
      pdadmin sec_master> user create -gsouser -no-password-policy taiuser
      "cn=taiuser,ou=websphere,o=ibm,c=us" taiuser taiuser ptaiuser
      pdadmin sec_master> user modify taiuser password-valid yes
      pdadmin sec_master> user modify taiuser account-valid yes
      ```

   d. In the WebSEAL configuration file *webseal_install_directory*/etc/
      webseald-default.conf, set the following parameter:

      ```
      basicauth-dummy-passwd=webseal_userid_passwd
      ```

      For example, if you set the taiuser/ptaiuser in Tivoli Access Manager, set
      the following parameter:basicauth-dummy-passwd = ptaiuser

      If you are using a form-based authentication, set the following parameters:

      ```
      forms-auth=both
      ba-auth=none
      ```

3. Configure WebSEAL with your product application server by enabling the
   TAI++ interceptor on the server.

   a. In the administrative console, select **Global security → Authentication
      mechanisms and expiration**.

b. Expand **Web and SIP security**, and then select **Trust Association**. Select the check box and click **Apply**.

c. Select **Interceptors** → **TAMTrustAssociationInterceptorPlus** → **custom properties**, and add the following properties:

Name	Value
com.ibm.websphere.security.webseal.configURL	${WAS_INSTALL_ROOT}/java/jre/PdPerm.properties
com.ibm.websphere.security.webseal.id	iv-creds
com.ibm.websphere.security.webseal.loginId	taiuser (if the user taiuser/ptaiuser was created in the Tivoli Access Manager)

d. Restart the cell.

e. To access the client, go to https://*webseal_server_name:webseal_port/junction name/web_uri_for_client*.

4. Configure the host junctions for your environment, so that the Business Space widgets appear. Complete one of the following steps, depending on whether you are using virtual host junctions or transparent host junctions.

- If you are using virtual host junctions, create a virtual host junction. A virtual host junction eliminates the need to create separate junctions.

   a. Make sure that a virtual host has been configured. Virtual host junctions match a host and port number and forward addresses to the target host. No URL filtering occurs, and all requests that match are forwarded to the target host.

   b. Make sure that the following applications are available to the same virtual host. You may have some or all of the applications, based on which products you are using with Business Space.

      – BPMAdministrationWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus and WebSphere Process Server)

      – BusinessSpaceHelpEAR_*nodename_servername* (for all products)

      – BSpaceEAR_*nodename_servername* (for all products)

      – BSpaceWebformsEnabler_*nodename_servername* (for all products)

      – HumanTaskManagementWidgets_*nodename_servername* (for WebSphere Process Server and WebSphere Business Monitor)

      – REST Services Gateway (for all products)

      – REST Services Gateway Dmgr (for WebSphere Enterprise Service Bus and WebSphere Process Server)

      – mm.was_*nodename_servername* (for all products)

      – WBMDashboardWeb_*nodename_servername* (for WebSphere Business Monitor)

      – wesbWidgets_*nodename_servername* (for WebSphere Enterprise Service Bus)

      – widgets_busleader_*nodename_servername* (for WebSphere Business Compass)

      – widgets_pubserver_*nodename_servername* (for WebSphere Business Compass)

      – widgets_fabric_*nodename_servername* (for WebSphere Business Services Fabric)

Note: This list of applications covers only the applications required by Business Space. You might need to add other applications to the list for non-Business Space scenarios using Tivoli Access Manager WebSEAL.

c. Run the following command using pdadmin: `server task webseal server virtualhost create -t transport -h target_host [-p port] [-v virtual_host_name] virtual_host_label`

Use the following information:

- *webseal server* is the name of the WebSEAL server where you will create the virtual host entry.
- *transport* is the type of transport. Valid entries are `tcp`, `ssl`, `tcpproxy`, and `sslproxy`.
- *target_host* is the host of the required application.
- *virtual_host_name* is used to match HTTP requests to a virtual host junction. If no value is entered, it is made up of the target host and port by default. For example, if you set the *virtual_host_name* to `myvirthost.ibm.com:80`, WebSEAL matches the URLs containing `myvirthost.ibm.com:80` and routes it to the host provided in the pdadmin command.
- *virtual_host_label* is the label used to identify the entry in WebSEAL. It must be unique.

For Business Space to run as expected, both `ssl` and `tcp` entries must be created for the type of transport. When you need both Secure Sockets Layer (SSL) and Transmission Control Protocol (TCP) to be supported in the same virtual host junction, you must us the -g *vhost_label* option, where *vhost_label* is the original virtual host label to share configuration. This option finds a previously created virtual host junction (one created earlier, where the *virtual_host_label* matches the label provided in the -g option), and will share that configuration. The second entry still needs its own *virtual_host_label*, but it can share the target host, port, and other values. If you do not provide this -g option, a second virtual host cannot be created because WebSEAL will see the target host and port as being identical to a previously create junction (which is not allowed).

- If you are using transparent host junctions, create a series of transparent path junctions for the widgets for each product.

a. Run the following command using pdadmin: `server task webseal server create -t transport type (ssl) or (tcp) -x -h hostname path`

For example, type: `server task webseald-default create -t tcp -x -h monServer.ibm.com /BusinessSpace`.

b. Create the following context roots for your product: Mapping Business Space URLs for a reverse proxy server.

5. Complete additional configuration steps to resolve issues with browser cookies and virtual hosts.

a. To resolve renaming of the Business Space cookie, add the following content to the WebSEAL configuration file:

`[preserve-cookie-names]`

`name = com.ibm.bspace.UserName`

`name = com.ibm.wbimonitor.UserName`

b. Optional: If you are using non-default virtual hosts with a context root, you might encounter issues with Business Space pages. You might need to stop the junction from rewriting the JavaScript on the Business Space pages by adding the -j junction to the context root. Run the following command:

```
server task default-webseald create -f -h hostname -p portnumber -t
tcp -b supply -c iv-user,iv-creds,iv-groups -x -s -j -J trailer/root
context
```

Assigning the Business Space superuser role

In Business Space, you can assign users to be superusers (or Business Space administrators). A superuser can view, edit, and delete all spaces and pages, can manage and create templates, and can change ownership of a space by changing the owner ID.

Before you begin

If administrative security is enabled when you configure Business Space, consider the following information about groups and superusers:

- Users belonging to the special user group, **administrators**, have a superuser role by default. As a result, the superuser role assignment is handled by user group membership.
- In a single-server environment, the Business Space server creates the **administrators** user group in the default user registry. The administrator ID provided during configuration is automatically added as member of this group.
- In a network deployment environment, the **administrators** user group is not created automatically. Use the createSuperUser.py script to create the user group and add members to that group in the default user registry.
- If another user registry (for example, LDAP) is used instead of the default user registry, or if the default user registry is used but you do not want to use the **administrators** user group, you must identify the user group that you are using for the Business Space superusers. Make sure that the value you provide can be understood by the user registry. For example, for LDAP, you might provide a name like cn=administrators,dc=company,dc=com. For more information about identifying this user group, see the instructions for changing the administrators group in the What to do next section.
- For Business Space in WebSphere Portal, the default group **wpsadmins** is also used for the superuser role. Members of this group are granted the superuser role for Business Space.

  Note: Security must be enabled if you want to use Business Space in WebSphere Portal.

If administrative security is not enabled when you configure Business Space, only the special user ID **BPMAdministrator** has the Business Space superuser role.

If you have a network deployment environment, you must run the createSuperUser.py script to assign the superuser role: to create the user group and add members. Before you run the script, complete the following steps:

- Make sure the default **administrators** group name is not changed.
- Use the default repository for the user registry.
- Start the server or the deployment manager for your Business Space environment for the profile where is Business Space installed.

Procedure

1. Locate the script *install_root*\BusinessSpace\scripts\createSuperUser.py for assigning the superuser role to a user.

2. Open a command prompt, and change directories to the following directory: *profile_root*\bin, where *profile_root* represents the directory for the profile where is Business Space installed.

3. Type the following command: wsadmin -lang jython -f *install_root*\ BusinessSpace\scripts\createSuperUser.py *user_short_name password* where *user_short_name* is the unique identifier for a user in Virtual Member Manager (VMM), and *password* is the VMM password for that user. If that user exists in VMM, the user is added to the administrator group.

   Note: When the path contains a space, for example, if *install_root* is My install dir, you must enclose the path names in quotation marks. For example, type the following command: wsadmin -lang jython -f "\My install dir\BusinessSpace\scripts\createSuperUser.py" *user_short_name_in_VMM*.

What to do next

To open Business Space, use the following URL: http://*host*:*port*/BusinessSpace, where *host* is the name of the host where your server is running and *port* is the port number for your server.

You can change the default special user group named **adminstrators**. Perform the following steps to check the current group name or change it to other name.

Inspect the value for the metric com.ibm.mashups.adminGroupName in the configuration file:

- *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ ConfigService.properties on a stand-alone server, or
- *deployment_manager_profile_root*\BusinessSpace*cluster_name*\ mm.runtime.prof\config\ConfigService.properties on a cluster.

If you want to change an administrative group, perform the following steps on a stand-alone server:

1. Modify the metric com.ibm.mashups.adminGroupName in the configuration file *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ ConfigService.properties.

2. Run the command updatePropertyConfig in the wsadmin environment of the profile:$AdminTask updatePropertyConfig {-serverName *server_name* -nodeName *node_name* -propertyFileName "*profile_root*\BusinessSpace*node_name*\ *server_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} and run $AdminConfig save.

3. Restart the server.

If you want to change an administrative group, perform the following steps on a cluster:

1. Modify the metric com.ibm.mashups.adminGroupName in the configuration file *deployment_manager_profile_root*\BusinessSpace*cluster_name*\ mm.runtime.prof\config\ConfigService.properties.

2. Run the command updatePropertyConfig in the wsadmin environment of the deployment environment profile:$AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\ mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} and run $AdminConfig save.

3. Restart the deployment manager.

If you want to change the superuser when security is not enabled, perform the following steps on a stand-alone server:

1. Modify the metric noSecurityAdminInternalUserOnly in the configuration file *profile_root*\BusinessSpace*node_name**server_name*\mm.runtime.prof\config\ ConfigService.properties.

2. Run the command updatePropertyConfig in the wsadmin environment of the profile:$AdminTask updatePropertyConfig {-serverName *server_name* -nodeName *node_name* -propertyFileName "*profile_root*\BusinessSpace*node_name*\ *server_name*\mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} and run $AdminConfig save.

3. Restart the server.

If you want to change the superuser when security is not enabled, perform the following steps on a cluster:

1. Modify the metric noSecurityAdminInternalUserOnly in the configuration file *deployment_manager_profile_root*\BusinessSpace*cluster_name*\ mm.runtime.prof\config\ConfigService.properties.

2. Run the command updatePropertyConfig in the wsadmin environment of the deployment environment profile:$AdminTask updatePropertyConfig {-clusterName *cluster_name* -propertyFileName "*deployment_manager_profile_root*\BusinessSpace*cluster_name*\ mm.runtime.prof\config\ConfigService.properties" -prefix "Mashups_"} and run $AdminConfig save.

3. Restart the deployment manager.

Commands (wsadmin scripting) for configuring Business Space

Look up a scripting object or command class to find details about its command syntax.

To open the information center table of contents to the location of this reference information, click the **Show in Table of Contents** button ( ) on your information center border.

configureBusinessSpace command

Use the configureBusinessSpace command to configure the database for Business Space powered by WebSphere.

This command configures the data source for Business Space and generates the scripts that create and configure database tables.

Required parameters

-serverName *server_name*
  A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *node_name*
  A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-clusterName *cluster_name*

A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

Optional parameters

-schemaName *schema_name*

An optional parameter that specifies the database schema for the Business Space database configuration. The default value is `IBMBUSSP`.

-tablespaceDir *table_space_path*

An optional parameter that specifies a directory path or file name prefix for the files used as the physical locations of table spaces. The default value is `BSP`. Valid for DB2, Oracle and SQL Server (otherwise ignored). For SQL Server, this parameter applies to the primary data file and log files.

-tablespaceNamePrefix *table_space_prefix*

An optional parameter that specifies a prefix string added to the beginning of table space names to make them unique. The default value is `BSP`. If a table space name prefix is longer than four characters, it is truncated to four characters. Valid for DB2, DB2 z/OS V8, DB2 z/OS V9, and Oracle (otherwise ignored).

-dbLocationName *database_location_name*

An optional parameter that specifies the database location name on z/OS. The default value is `BSP` or the product database name. Valid on DB2 z/OS V8 and V9 (otherwise ignored).

-storageGroup *storage_group*

An optional parameter that specifies the storage group on z/OS for Business Space. If you are using z/OS, you must update the database scripts that are generated before running them. For more information about the scripts, see "Configuring Business Space database tables."

-bspacedbDesign *database_design_file_name*

An optional parameter that specifies a database design file that you are using to define all database configuration information, including the schema, and the table space directory. If you designate a database design file using the **-bspacedbDesign** parameter, you do not need to designate the **-schemaName**, **-tablespaceDir** , or **-storageGroup** parameters, unless you want to override what is in the database design file for particular database configuration information.

Note: The JNDI name of jdbc/mashupDS is always used for a Business Space data source, so the JNDI name in the database design file is not used. If a data source with a JNDI name of jdbc/mashupDS exists, this command stops without configuring the profile unless you also specify the `-replaceDatasource true` parameter.

-productTypeForDatasource *product_database*

An optional parameter that specifies properties to use to create the data source to use with Business Space. Designating a **productTypeForDatasource** creates a data source for Business Space with a JNDI name of jdbc/mashupDS that is modeled on the data source of an installed product, such as WebSphere Process Server, WebSphere Enterprise Service Bus, WebSphere Business Monitor, and WebSphere Business Compass. Valid values are `WPS` (to designate WebSphere Process Server or WebSphere Enterprise Service Bus), `WPBS` (to designate WebSphere Business Compass), and `WBM` (to designate WebSphere Business Monitor). If the **bspacedbDesign** parameter is also specified, the

productTypeForDatasource overrides the database type and JDBC provider, and the JNDI name in the database design file is not used.

Note: If a data source with a JNDI name of jdbc/mashupDS exists, this command stops without configuring the profile unless you also specify the `-replaceDatasource true` parameter.

-replaceDatasource true|false
An optional parameter that specifies whether the configureBusinessSpace command runs if the profile has already been configured. The default value is `false`. When a profile is configured for Business Space, a data source with a JNDI name of jdbc/mashupDS is created. If the data source exists and you run the configureBusinessSpace command without specifying `-replaceDatasource true`, the command does not change the configuration. If you specify `true`, the command deletes the data source and its JDBC provider, creates new ones, and creates new DDL scripts.

–save true|false
A parameter that indicates saving your configuration changes. The default value is `false`.

Examples

The following example uses the configureBusinessSpace command to configure a Business Space data source on a server.

- Jython example:

```
AdminTask.configureBusinessSpace('[-nodeName myNode -serverName
 myServer']')
```

- Jacl example:

```
$AdminTask configureBusinessSpace {-nodeName myNode -serverName
 myServer}
```

The following example uses the configureBusinessSpace to configure a Business Space data source on a cluster and save the changes.

- Jython example:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster -save
 true]')
```

- Jacl example:

```
$AdminTask configureBusinessSpace {-clusterName myCluster -save
 true}
```

The following example uses the configureBusinessSpace to configure a Business Space data source on a cluster, with a schema name and a product data source designated for WebSphere Process Server.

- Jython example:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster
 -schemaName myCluster -productTypeForDatasource WPS -save true]')
```

- Jacl example:

```
$AdminTask configureBusinessSpace {-clusterName myCluster
 -schemaName myCluster -productTypeForDatasource WPS -save true}
```

The following example uses the configureBusinessSpace to configure a Business Space data source on a cluster using database information that is in the database design file.

- Jython example:

```
AdminTask.configureBusinessSpace('[-clusterName myCluster
 -bspacedbDesign "C:\BSpace_dbDesign.properties" -save true]')
```
- Jacl example:
```
$AdminTask configureBusinessSpace {-clusterName myCluster
 -bspacedbDesign "C:\BSpace_dbDesign.properties" -save true}
```

configureLotusWebformServer command

Use the configureLotusWebformServer command to configure Business Space to
use IBM Lotus WebForm Server. Lotus Webform Server works with Human Task
Management widgets and applies to WebSphere Process Server servers and clusters
and any business process management product installation that includes
WebSphere Process Server.

The configureLotusWebformServer command configures Business Space to use IBM
Lotus WebForm Server to work with Human Task Management widgets. Webform
Server must be installed on the same machine where you are running the script.

Required parameters

-serverName *server_name*
    A parameter that specifies the server name for the configuration. For
    configuring Business Space widgets on a server, you must specify both a
    serverName and a **nodeName**.

-nodeName *node_name*
    A parameter that specifies the node name for the configuration. Either a
    serverName, nodeName, or clusterName is required. For configuring on a
    server, you must specify both a **serverName** and a **nodeName**.

-clusterName *cluster_name*
    A parameter that specifies the cluster name for the configuration. For
    configuring Business Space on a cluster, you must specify a **clusterName**.

–translatorHTTPLocation *URL*
    A parameter that specifies the location of the Webform Server Translator. The
    default URL for the location is `http://localhost:8085/translator`.

-serverInstallRoot *Webform_Server_install_root*
    A parameter that specifies the full path where Lotus Webform Server is
    installed. For example, the Lotus Webform Server install root might be
    `C:/IBM/LotusWebForms/3.5/WebFormServer`

Optional parameters

-save true|false
    A parameter that indicates saving your configuration changes. The default
    value is `true`.

Examples

The following example uses the configureLotusWebformServer to configure
Business Space to use Lotus WebForm Server with the Human Task Management
widgets.
- Jython example:
```
AdminTask.configureLotusWebformServer('[-nodeName node_name
 -serverName server_name -translatorHTTPLocation
 http://localhost:9080/translator -serverInstallRoot
 C:/IBM/LotusWebForms/3.5/WebFormServer]')
```
- Jacl example:

```
$AdminTask configureLotusWebformServer {-nodeName node_name
 -serverName server_name -translatorHTTPLocation
 http://localhost:9080/translator
 -serverInstallRoot C:/IBM/LotusWebForms/3.5/WebFormServer}
```

getBusinessSpaceDeployStatus command

Use the getBusinessSpaceDeployStatus command to check whether Business Space powered by WebSphere is configured on a particular deployment target.

This command checks whether Business Space is configured on a server, node, or cluster that you specify. If you don't set any parameters, it checks if Business Space is configured in the cell.

Required parameters

-serverName *server_name*
  A parameter that specifies the server name to check for Business Space.

-nodeName *node_name*
  A parameter that specifies the node name to check for Business Space.

-clusterName *cluster_name*
  A parameter that specifies the cluster name to check for Business Space.

Examples

The following example uses the getBusinessSpaceDeployStatus command to check whether Business Space is configured on a server.

- Jython example:

  ```
  AdminTask.getBusinessSpaceDeployStatus('[-nodeName myNode -serverName
   myServer]')
  ```

- Jacl example:

  ```
  $AdminTask getBusinessSpaceDeployStatus {-nodeName myNode -serverName
  myServer}
  ```

The following example uses the getBusinessSpaceDeployStatus command to check whether Business Space is configured on a cluster.

- Jython example:

  ```
  AdminTask.getBusinessSpaceDeployStatus('[-clusterName myCluster]')
  ```

- Jacl example:

  ```
  $AdminTask getBusinessSpaceDeployStatus {-clusterName myCluster}
  ```

The following example uses the getBusinessSpaceDeployStatus command to return a list of all deployment targets (server and clusters) configured for Business Space in a cell.

If you run the command from the profile root `bin` directory, the command returns a list of all deployment targets (server and clusters) configured for Business Space in a cell.

If you run the command from the installation root `bin` directory, the command returns a list of all deployment targets (server and clusters) configured for Business Space in the same installation root directory.

- Jython example:

  ```
  AdminTask.getBusinessSpaceDeployStatus()
  ```

- Jacl example:

```
$AdminTask getBusinessSpaceDeployStatus
```

installBusinessSpace command

Use the installBusinessSpace command to set up Business Space powered by WebSphere on your runtime environment.

The installBusinessSpace command installs the Business Space enterprise archive (EAR) files in your runtime environment.

Required parameters

-serverName *server_name*
> A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *node_name*
> A parameter that specifies the node name for the configuration. Either a serverName, nodeName, or clusterName is required. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-clusterName *cluster_name*
> A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

Optional parameters

–noWidgets true|false
> An optional parameter that if set to `true` prevents the product widgets from being installed on the deployment target. Then, if you want to install widgets, you must use the installBusinessSpaceWidgets command after the Business Space configuration has completed successfully. The default value is `false`.

–save true|false
> An optional parameter that indicates saving your configuration changes. The default value is `false`.

Examples

The following example uses the installBusinessSpace command to install Business Space EAR files on a server.

- Jython example:
  ```
  AdminTask.installBusinessSpace('[-nodeName myNode -serverName
   myServer -save true]')
  ```
- Jacl example:
  ```
  $AdminTask installBusinessSpace {-nodeName myNode -serverName
   myServer -save true}
  ```

The following example uses the installBusinessSpace to install Business Space EAR files on a cluster.

- Jython example:
  ```
  AdminTask.installBusinessSpace('[-clusterName myCluster -save true]')
  ```
- Jacl example:
  ```
  $AdminTask installBusinessSpace {-clusterName myCluster -save true}
  ```

installBusinessSpaceWidgets command

Use the installBusinessSpaceWidgets command to install, deploy and register widgets for use with Business Space powered by WebSphere.

The installBusinessSpaceWidgets command installs, deploys, and registers designated widgets contained in a compressed file or an enterprise archive (EAR) file. If widgets are already deployed, the installBusinessSpaceWidgets command refreshes the binary and registration information.

The structure of the widget compressed file contains the following items:
- [ear\widgets_*name*.ear] one or more EAR files.
- [catalog\catalog_*name*.xml]
- [endpoints*.xml] widget endpoints
- [templates*.zip] Templates must be in a compressed file and follow IBM Lotus Mashups template format.
- [help\eclipse\plugins*]

All folders are not required. Empty folders are valid.

Required parameters

-serverName *server_name*
> A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *node_name*
> A parameter that specifies the node name for the configuration. Either a serverName, nodeName, or clusterName is required. For configuring Business Space widgets on a server, you must specify both a **serverName** and a **nodeName**.

-clusterName *cluster_name*
> A parameter that specifies the cluster name for the configuration. For configuring Business Space widgets on a cluster, you must specify a **clusterName**.

-widgets *widgets_path*
> A parameter that specifies one of the following:
> - the full path for the directory that contains the compressed files or the EAR files that contain the widgets. If you specify a directory, all widgets will be installed for all compressed files and EAR files in that directory.
> - the full path to an individual compressed file that contains the widgets.
> - the full path to an individual EAR file that contains the widgets.

–save true|false
> A parameter that indicates saving your configuration. The default value is `true`.

Optional parameters

–save true|false
> A parameter that indicates saving your configuration. The default value is `true`.

Examples

The following example uses the installBusinessSpaceWidgets to install, deploy, and register widgets on a server.

- Jython example:

```
AdminTask.installBusinessSpaceWidgets('[-nodeName node_name
  -serverName server_name -widgets
  install_root\BusinessSpace\widgets\MyWidget.zip]')
```

- Jacl example:

```
$AdminTask installBusinessSpaceWidgets {-nodeName node_name
  -serverName server_name -widgets
  install_root\BusinessSpace\widgets\MyWidget.zip}
```

The following example uses the installBusinessSpaceWidgets to install, deploy, and register widgets on a cluster.

- Jython example:

```
AdminTask.installBusinessSpaceWidgets('[-clusterName cluster_name
  -widgets X:\WPS\Temp]')
```

- Jacl example:

```
$AdminTask installBusinessSpaceWidgets {-clusterName cluster_name
  -widgets X:\WPS\Temp}
```

Manual steps are required for updating Business Space templates and spaces after running the installBusinessSpaceWidgets or updateBusinessSpaceWidgets command. For more information, see Updating Business Space templates and spaces after installing or updating widgets.

registerRESTServiceEndpoint command

Use the registerRESTServiceEndpoint command to register configured and enabled Representational State Transfer (REST) endpoints so that your team can use the widgets in Business Space.

This command registers the REST service endpoints so that Business Space is properly connected to widgets for your product. This command registers the endpoints of the REST services that are in the same cell as Business Space.

Required parameters

-clusterName *name_of_rest_services_cluster*
> A parameter that specifies the cluster name for the REST service. When registering REST services endpoints for a cluster, you must specify a **clusterName**.

-nodeName *name_of_rest_services_node*
> A parameter that specifies the node name for the REST service. When registering REST services endpoints for a server, you must specify both a **serverName** and a **nodeName**.

-serverName *name_of_rest_services_server*
> A parameter that specifies the server name for the REST service. When registering REST services endpoints for a server, you must specify both a **serverName** and a **nodeName**.

-businessSpaceClusterName *name_of_business_space_cluster*
> The Business Space cluster name. If Business Space is configured on a cluster, you must specify a **businessSpaceClusterName**.

-businessSpaceNodeName *name_of_business_space_node*

    The Business Space node name. If Business Space is configured on a server, you must specify both a **businessSpaceServerName** and a **businessSpaceNodeName**.

-businessSpaceServerName *name_of_business_space_server*

    The Business Space server name. If Business Space is configured on on a server, you must specify both a **businessSpaceServerName** and a **businessSpaceNodeName**.

Optional parameters

-appName *name_of_provider_application*

    The application name of the REST service provider.

-type *name_of_service_type*

    The type of the service. This parameter is optional. If this parameter is not specified, all unique REST service endpoints configured for a specified REST service provider on a specified deployment target are registered. If you want to specify a specific service endpoint, use the `<tns:type>` value that is in the endpoints file for a widget. The endpoints files are located at `install_root\BusinessSpace\registryData\endpoints` directory. For example, `bpmAdministrationEndpoints.xml` contains all service endpoint types that are used by Administration widgets. The value of the `<tns:type>` element is `{com.ibm.bpm}SCA`:

```
<tns:Endpoint>
    <tns:id>{com.ibm.bpm}SCA</tns:id>
    <tns:type>{com.ibm.bpm}SCA</tns:type>
    <tns:version>6.2.0.0</tns:version>
    <tns:url>/rest/sca/v1</tns:url>
    <tns:description>Location backend SCA REST Services
 for Module Administration widgets and Service Monitoring widget
</tns:description>
  </tns:Endpoint>
```

    For Jacl, make sure to use double quotes around the value, for example: `... -type "{com.ibm.bpm}SCA" ...`.

-webModuleName *name_of_web_module*

    The web module name of the REST service provider.

-version *name_of_version*

    The version of the REST service provider.

Examples

The following example uses the registerRESTServiceEndpoint command. It registers all configured and enabled REST services on the cluster with Business Space.

- Jython example:

```
AdminTask.registerRESTServiceEndpoint('[-clusterName
 name_of_rest_services_cluster -businessSpaceClusterName
 name_of_business_space_cluster]')
```

- Jacl example:

```
$AdminTask registerRESTServiceEndpoint {-clusterName
 name_of_rest_services_cluster -businessSpaceClusterName
 name_of_business_space_cluster}
```

uninstallBusinessSpaceWidgets command

Use the uninstallBusinessSpaceWidgets command to remove widgets and widget definitions from the profile, including removing individual widget assets (application, catalog, endpoints, spaces, templates, help).

The uninstallBusinessSpaceWidgets command removes widget files in a designated compressed file or an enterprise archive (EAR) file. The structure of the widget compressed file contains the following items:

- [ear\widgets_*name*.ear] one or more EAR files.
- [catalog\catalog_*name*.xml]
- [endpoints*.xml] widget endpoints
- [templates*.zip] Templates must be in a compressed file and follow IBM Lotus Mashups template format.
- [help\eclipse\plugins*]

All folders are not required. Empty folders are valid.

Note: If you customized REST endpoint information outside of using the updateBusinessSpaceWidgets command, those endpoint changes are lost after running the uninstallBusinessSpaceWidgets command.

Required parameters

-serverName *server_name*
> A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *node_name*
> A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-clusterName *cluster_name*
> A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

-widgets *widgets_path*
> A parameter that specifies one of the following:
> - the full path for the directory that contains the compressed files or the widget EAR files that contain the widgets. If you specify a directory, all widgets will be installed for all compressed files and EAR files in that directory.
> - the full path to an individual compressed file that contains the widgets.
> - the full path to an individual EAR file that contains the widgets.

Optional parameters

–save true|false
> A parameter that indicates saving your configuration changes. The default value is `true`.

Example

The following example uses the uninstallBusinessSpaceWidgets command to remove widgets from a cluster.

- Jython example:

```
AdminTask.uninstallBusinessSpaceWidgets('[-clusterName
 cluster_name -widgets X:\WPS\Temp]')
```
- Jacl example:
```
$AdminTask uninstallBusinessSpaceWidgets {-clusterName
cluster_name -widgets X:\WPS\Temp}
```

updateBusinessSpaceWidgets command

Use the updateBusinessSpaceWidgets command to update previously configured Business Space widgets and their endpoints, catalogs, templates, and help plugins.

The updateBusinessSpaceWidgets command updates widget binary files, catalog files, endpoint files, templates, and help plug-ins for widgets that have been previously installed and configured for Business Space.

The updateBusinessSpaceWidgets command updates widget files in a designated compressed file or an enterprise archive (EAR) file. The structure of the widget compressed file contains the following items:

- [ear\widgets_*name*.ear] one or more EAR files.
- [catalog\catalog_*name*.xml]
- [endpoints*.xml] widget endpoints
- [templates*.zip] Templates must be in a compressed file and follow IBM Lotus Mashups template format.
- [help\eclipse\plugins*]

All folders are not required. Empty folders are valid.

Required parameters

-serverName *server_name*
> A parameter that specifies the server name for the configuration. For configuring Business Space widgets on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *node_name*
> A parameter that specifies the node name for the configuration. Either a serverName, nodeName, or clusterName is required. For configuring Business Space widgets on a server, you must specify both a **serverName** and a **nodeName**.

-clusterName *cluster_name*
> A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

Optional parameters

-widgets *widget_path*
> A parameter that specifies the full path for the directory where widget enterprise archive (EAR) files or widget compressed files are located or the full path to a specific EAR file or widget compressed file.

-endpoints *endpoint_path*
> A parameter that specifies the full path for the directory where the widget endpoint files are located or the full path to a specific endpoint file.

-catalogs *catalog_path*
> A parameter that specifies the full path for the directory that contains the widget catalog files or the full path to a specific catalog file.

-templates *template_path*

A parameter that specifies the full path for the directory that contains the widget template files or the full path to a specific template file.

-helpplugins *help_path*

A parameter that specifies the full path for the directory that contains the widget online help plugin files or the full path to a specific widget online help plugin file.

–noWidgets true|false

Specifies that you do not want to update the widget EAR files that are contained within the widgets compressed file.

–noEndpoints true|false

Specifies that you do not want to update the specified endpoint files that are contained in the widgets compressed file.

–noCatalogs true|false

Specifies that you do not want to update the catalog definition files that are contained in the widgets compressed file.

–noTemplates true|false

Specifies that you do not want to update the templates that are contained in the widgets compressed file.

–noHelp true|false

Specifies that you do not want to update the help files that are contained in the widgets compressed file.

–save true|false

A parameter that indicates saving your configuration. The default value is `true`.

Examples

The following example uses the updateBusinessSpaceWidgets to update widgets on a cluster.

Jacl example:Jython example:

```
AdminTask.updateBusinessSpaceWidgets('[-clusterName cluster_name
 -widgets widget_path]')
```

```
$AdminTask updateBusinessSpaceWidgets {-clusterName cluster_name
 -widgets  widget_path}
```

The following example uses the updateBusinessSpaceWidgets to update widgets on a server.

Jython example:

```
AdminTask.updateBusinessSpaceWidgets('[-nodeName node_name
-serverName server_name -widgets widget_path]')
```

Jacl example:

```
$AdminTask updateBusinessSpaceWidgets {-nodeName node_name
 -serverName server_name -widgets  widget_path}
```

Manual steps are required for updating Business Space templates and spaces after running the installBusinessSpaceWidgets or updateBusinessSpaceWidgets command. For more information, see Updating Business Space templates and spaces after installing or updating widgets.

updateRESTGatewayService command

Use the updateRESTGatewayService command to update a Representational State Transfer (REST) gateway service so that REST services are configured and enabled.

This command updates the REST Gateway service so that REST services are configured and enabled. The deployment of the REST services is performed automatically in a stand-alone server profile. For other types of configurations, the REST Services administrative console page or the updateRESTGatewayService allows you to configure REST services for all of your product's widgets in Business Space.

Note: For WebSphere Process Server, Business Process Choreographer and Human Task Management REST services are configured when you configure the Business Process Choreographer and Human Task Management containers.

Required parameters

-clusterName *cluster_name*
> A parameter that specifies the cluster name for the REST service. For configuring REST services on a cluster, you must specify a **clusterName**.

-nodeName *node_name*
> A parameter that specifies the node name for the REST service. For configuring REST services on a server, you must specify both a **serverName** and a **nodeName**.

-serverName *server_name*
> A parameter that specifies the server name for the REST service. For configuring REST services on a server, you must specify both a **serverName** and a **nodeName**.

-enable true | false
> Indicates if the REST service is enabled. Valid values include `true` or `false`.

Optional parameters

-type *name_of_service_type*
> The type of the REST service.

-version *name_of_version*
> The version of the REST service.

Examples

The following example uses the updateRESTGatewayService command to update the REST Gateway service so that REST services are configured and enabled.

- Jython example:

```
AdminTask.updateRESTGatewayService('[-nodeName node1 -serverName
  server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable
  true]')
```

- Jacl example:

```
$AdminTask updateRESTGatewayService {-nodeName node1 -serverName
  server1 -type "{com.ibm.bpm}TimeTable" -version 6.2.0.0 -enable true}
```

Updating Business Space templates and spaces after installing or updating widgets

Manual steps are required for updating Business Space templates and spaces after running the installBusinessSpaceWidgets or updateBusinessSpaceWidgets commands in a clustered environment.

Before you begin

You must complete the following additional steps if you have previously used the installBusinessSpaceWidgets command or the updateBusinessSpaceWidgets command.

Procedure

1. If Business Space is configured in a cluster, perform the following steps:
   a. Identify the custom profile for `oobLoadedStatus` properties file:
      1) In deployment manager profile, open the `deployment_manager_profile_root\BusinessSpace\cluster_name\ mm.runtime.prof\config\ConfigService.properties` file.
      2) Look for the name of cell, node and server in the `com.ibm.mashups.directory.templates` or `com.ibm.mashups.directory.spaces` properties.

         For example, in `com.ibm.mashups.directory.templates = config/cells/Cell01/nodes/Node01/servers/Server1/mm/templates`, you can locate the custom profile by the `Cell01` cell name and the `Node01` node name.
      3) Use the name of cell, node and server to locate the custom profile.
   b. In the custom profile, open the `custom_profile_root\BusinessSpace\ cluster_name\mm.runtime.prof\public\oobLoadedStatus.properties` file and update the `importTemplates.txt` or `importSpaces.txt` properties:

      ```
      importTemplates.txt=true
      importSpaces.txt=true
      ```
   c. Resynchronize the custom profile.
      1) Open the administrative console and click **System administration → Nodes**.
      2) Click **Full Resynchronize**.
   d. Restart the cluster.
2. If Business Space is configured in a managed server, perform the following steps:
   a. In the custom profile where the managed server is located, open the `custom_profile_root\BusinessSpace\node_name\server_name\ mm.runtime.prof\public\oobLoadedStatus.properties` file and update the `importTemplates.txt` or `importSpaces.txt` properties:

      ```
      importTemplates.txt=true
      importSpaces.txt=true
      ```
   b. Resynchronize the custom profile.
      1) Open the administrative console and click **System administration → Nodes**.
      2) Click **Full Resynchronize**.
   c. Restart the server.

Configuring Business Space on WebSphere Portal

If your team uses WebSphere Portal, you can configure Business Space to work in the WebSphere Portal environment.

Before you begin

Before you complete this task, you must have completed the following tasks:

- Installed and configured WebSphere Portal V6.1.0.3 with feature pack V6.1.5.
- Installed your WebSphere business process management product (WebSphere Business Compass, WebSphere Business Monitor, WebSphere Business Services Fabric, WebSphere Enterprise Service Bus, or WebSphere Process Server).
- Configured Representational State Transfer (REST) services, so widgets can access the services during run time.
- Completed specific configuration steps for your widgets, if required.

For an administration installation of WebSphere Portal: If during the installation of your portal you selected the administration installation option and you want to use Business Space on WebSphere Portal, you must enable mashup integration, add the new mashup root page, and configure access control. Complete the following steps:

1. Open a command prompt and navigate to the directory `wp_profile_root\ConfigEngine`.
2. Run the following configuration task

   ```
   ConfigEngine.sh|bat deploy-portal-mashup-ui
                   -DWasPassword=was_password
                   -DPortalAdminPwd=portal_password
   ```

   If you add passwords to the wkplc.properties file located in the `wp_profile_root\ConfigEngine\properties` directory, you do not need to specify the passwords on the command line. This script creates a top- level page named My Mashups next to the Home node.
3. Configure access control settings for mashups in your portal as described in the WebSphere Portal documentation.

When you set up Business Space widgets to work in WebSphere Portal, consider the following issues:

- Do not install a business process management product on a WebSphere Portal server.
- You cannot mix other WebSphere Portal portlets and the Business Space widgets on the same page.

Follow one of the following procedures to set up Business Space on WebSphere Portal for either a server or a clustered environment.

Configuring Business Space on a WebSphere Portal server

If your team uses WebSphere Portal, you can configure Business Space to work with a WebSphere Portal server.

Before you begin

Before you complete these steps, make sure you have completed the prerequisites described in Configuring Business Space on WebSphere Portal.

Procedure

1. Start the launchpad for your product and click **Add-in for WebSphere Portal** to run the Business Space on WebSphere Portal installer. For most business process management products, this option is available under **Additional software installation**. For WebSphere Business Compass, the option is available

under **Advanced Installation Options**. On the Business Space on WebSphere Portal installer, you can designate an automatic installation for a stand-alone server with a Derby database, or you can designate a custom installation for other configurations. Complete the installation using the Business Space on WebSphere Portal installer.

2. If you performed a custom installation, complete the following steps:

   a. Prepare a properties file. See the Example properties file for configuring WebSphere Portal.

   b. Edit *wp_profile*`\ConfigEngine\properties\wkplc.properties` and set the value for `WasPassword` to the administrative password for the WebSphere Application Server that you are using with WebSphere Portal, and the value for `PortalAdminPwd` to the administrative password for your WebSphere Portal product.

   c. Start the WebSphere Portal server (the **WebSphere_Portal** application) by running the `startServer.bat` file or the `startServer.sh` file from the *wp_profile*`\bin` directory.

   d. The default SOAP timeout of 180 seconds might not be long enough, because the administrative tasks do not begin until WebSphere Portal configuration tasks. Increase SOAP timeout by editing the *wp_profile*`\properties\soap.client.props` file and set the SOAP timeout as `com.ibm.SOAP.requestTimeout=1800`.

   e. Open a command prompt and change to the *wp_profile*`/bin` directory. Type the following command: `wsadmin -port` *SOAP_connector_address* `-user` *wsadmin_user_name* `-password` *wsadmin_password*.

      Here is an example of the command:

      ```
      C:\IBM\WebSphere\wp_profile\bin> wsadmin -port 10033 -user
        wasadmin -password wasadmin
      ```

      You can get the SOAP connector port by clicking **Application Servers** → **WebSphere_Portal** → **ports** → *SOAP_connector_address*.

   f. Restart the server.

   g. Run the installBusinessSpaceOnPortal command.

      Jython example: `AdminTask.installBusinessSpaceOnPortal('[-serverName` *WebSphere_Portal_server* `-nodeName` *WebSphere_Portal_node* `-user` *wsadmin_user_name* `-password` *wsadmin_password* `-portalRoot` *WebSphere_Portal_home*`]')`

      Jacl example: `$AdminTask installBusinessSpaceOnPortal {-serverName` *WebSphere_Portal_server* `-nodeName` *WebSphere_Portal_node* `-user` *wsadmin_user_name* `-password` *wsadmin_password* `-portalRoot` *WebSphere_Portal_home*`}`

      The *WebSphere_Portal_home* is where WebSphere Portal Server is installed, for example `C:\IBM\WebSphere\PortalServer`.

   h. Run the configureBusinessSpaceOnPortal command.

      Jython example: `AdminTask.configureBusinessSpaceOnPortal ('[-serverName` *WebSphere_Portal_server* `-nodeName` *WebSphere_Portal_node* `-inputParamsFile` *full_path_to_properties_file*`]')`

      Jacl example: `$AdminTask configureBusinessSpaceOnPortal {-serverName` *WebSphere_Portal_server* `-nodeName` *WebSphere_Portal_node* `-inputParamsFile` *full_path_to_properties_file*`}`

      For *full_path_to_properties_file*, use the properties file that you created in step 2.a.

i. Check for errors in the `SystemOut.log` file for the WebSphere Portal server. Specifically, look for errors that state `MANUALLY EDIT AND RUN THE COMMAND` or `build failed`. If any errors show the message `MANUALLY EDIT AND RUN THE COMMAND`, verify the command generated and run it manually. The full command is generated in the logs. Generally, these errors occur if the `wkplc.proprties` file has incorrect `WasPassword` and `PortalAdminPwd` information. Commands could also fail if you lack the needed file permissions when running the configuration.

j. Run the Business Space DDLs against your database. You can find them in *wp_profile*\dbscripts\BusinessSpace directory where they were generated. Review the generated DDL files before running the scripts.

Use the `configBusinessSpaceDB.bat` or `configBusinessSpaceDB.sh` script for your database, depending on your platform. For more information about running the database scripts, see Configuring Business Space database tables. If you run the scripts individually, they must be run manually in this order: `createDatabase.sql` (not needed if you want to use the same database as used by Portal Server), `createSchema.sql` (to create the Business Space schema), and `createTables_BusinessSpace.sql` (to create Business Space tables). For information about how to run a .sql script with your database, refer to the documentation for your database product.

3. Restart the WebSphere Portal server.

What to do next

If you performed a custom installation, run the installBusinessSpaceWidgetsOnPortal and the updateEndpointBindingOnPortal commands to set up your BPM widgets on WebSphere Portal.

1. Run the installBusinessSpaceWidgetsOnPortal command:

   Jython example: `AdminTask.installBusinessSpaceWidgetsOnPortal('[-serverName WebSphere_Portal_server_name -nodeName WebSphere_Portal_node_name -widgets install_root\BusinessSpace\widgets\MyWidget.zip -portalusername user_name -portalpassword password]')`

   Jacl example: `$AdminTask installBusinessSpaceWidgetsOnPortal {-serverName WebSphere_Portal_server_name -nodeName WebSphere_Portal_node_name -widgets install_root\BusinessSpace\widgets\MyWidget.zip -portalusername user_name -portalpassword password}`

2. Update the endpoints files for your product widgets, available at *WebSphere_Portal_application_server*/BusinessSpace/registryData/endpoints. For more information about your product-specific endpoints files, see Enabling Business Space widgets to work with multiple endpoints.

3. Run the updateEndpointBindingsOnPortal command:

   Jython example: `AdminTask.updateEndpointBindingsOnPortal ('[-serverName WebSphere_Portal_server_name  -nodeName WebSphere_Portal_node]')`

   Jacl example: `$AdminTask updateEndpointBindingsOnPortal {-serverName WebSphere_Portal_server_name -nodeName WebSphere_Portal_node}`

After you have configured Business Space for WebSphere Portal, you must complete the following tasks to get the Business Space environment in WebSphere Portal ready for your business users:

- Configure single sign-on (SSO) and the Secure Sockets Layer (SSL) certificates for your widgets. For more information, see Configuring SSO and SSL for widgets on WebSphere Portal.

- Create a space on WebSphere Portal for your widgets. For more information, see Creating a space on WebSphere Portal for your Business Space widgets.

Note: Business Space uses a proxy component to connect to your REST services. In some cases if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST service, depending on the performance of the REST service servers. If the REST service connections are timing out, update the following settings. By default, the socket-timeout value is set to 10 seconds. Change it to an appropriate value for your situation. If you are using WebSphere Process Server administration widgets, set the initial timeout value to 30 seconds.

1. Open the file *wp_profile*/installedApps/*node_name*/AJAX Proxy Configuration.ear/wp.proxy.config.war/WEB-INF/proxy-config.xml

2. Change the `proxy:value` for `socket-timeout`. The time is specified in milliseconds.

   ```
   <proxy:meta-data>
    <proxy:name>socket-timeout</proxy:name>
    <proxy:value>10000</proxy:value>
   </proxy:meta-data>
   ```

3. Log in to the administrative console for WebSphere Portal.

4. Restart the AJAX Proxy Configuration application.

Configuring Business Space on a WebSphere Portal cluster

If your team uses WebSphere Portal, you can configure Business Space to work with WebSphere Portal in a clustered environment.

Before you begin

Before you complete these steps, make sure you have completed the prerequisites described in Configuring Business Space on WebSphere Portal.

Procedure

1. On the primary node, start the launchpad for your product and click **Add-in for WebSphere Portal** to run the Business Space on WebSphere Portal installer. For most business process management products, this option is available under **Additional software installation**. For WebSphere Business Compass, the option is available under **Advanced Installation Options**. On the Business Space on WebSphere Portal installer, designate a custom installation and complete the installation using the Business Space on WebSphere Portal installer.

2. Install the V7.0.0.2 fix pack for your product on the primary node. For more information, see http://www.ibm.com/support/docview.wss?uid=swg21428093.

3. Start the node agent on the primary node.

4. Start the deployment manager.

5. Start the WebSphere Portal server on the primary node. Typically, this server name is **WebSphere_Portal**.

6. In order to capture details of any errors that might occur, use the following trace string: `*=info: com.ibm.bspace.*=all:com.ibm.mm.*=all`.

7. Prepare a properties file. See the Example properties file for configuring WebSphere Portal.

8. Edit *wp_profile*/ConfigEngine/properties/wkplc.properties and set the value for `WasPassword` to the administrative password for the WebSphere

Application Server that you are using with WebSphere Portal, and the value for `PortalAdminPwd` to the administrative password for your WebSphere Portal product.

9. Open a command prompt on the primary node and change to the *wp_profile*/bin directory. Type the following command: `wsadmin -port` *SOAP_connector_address* `-user` *wsadmin_user_name* `-password` *wsadmin_password* `-host` *primary_node_host_name*.

   You can get the SOAP connector port by clicking **Servers** → **Server clusters** → *name_of_cluster* → **Cluster members** → **WebSphere_Portal** → **ports** → *SOAP_connector_address*.

10. Run the installBusinessSpaceOnPortal command. Type the following command:

    Jython example: `AdminTask.installBusinessSpaceOnPortal('[-clusterName` *WebSphere_Portal_cluster* `-dmHost` *deployment_manager_host_name* `-dmPort` *deployment_manager_SOAP_port* `-dmUser` *deployment_manager_administrator_user_name* `-dmPassword` *deployment_manager_administrator_password* `-portalRoot` *WebSphere_Portal_home*`]')`

    Jacl example: `$AdminTask installBusinessSpaceOnPortal {-clusterName` *WebSphere_Portal_cluster* `-dmHost` *deployment_manager_host_name* `-dmPort` *deployment_manager_SOAP_port* `-dmUser` *deployment_manager_administrator_user_name* `-dmPassword` *deployment_manager_administrator_password* `-portalRoot` *WebSphere_Portal_home*`}`

    The *WebSphere_Portal_home* is where WebSphere Portal Server is installed, for example `C:/IBM/WebSphere/PortalServer`.

11. Run the configureBusinessSpaceOnPortal command with a properties file.

    Jython example: `AdminTask.configureBusinessSpaceOnPortal ('[-inputParamsFile` *full_path_to_properties_file*`]')`

    Jacl example: `$AdminTask configureBusinessSpaceOnPortal {-inputParamsFile` *full_path_to_properties_file*`}`

    For *full_path_to_properties_file*, use the properties file that you created in step 7.

12. Update the `AJAX Proxy Configuration.ear` application at the cluster scope, using the administrative console.

    a. Log in to the administrative console on the deployment manager.

    b. Click **Applications** → **Enterprise Applications**.

    c. Select **AJAX Proxy Configuration** and click **Update**.

    d. Under Application update options, click **Replace or add a single file**.

    e. In the **Specify the path beginning with the installed application archive file to the file to be replaced or added.**field, type `/wp.proxy.config.war/` `WEB-INF/proxy-config.xml`.

    f. Copy the *primary_node*`/wp_profile/installedApps/`*node_name*`/AJAX Proxy Configuration.ear/wp.proxy.config.war/WEB-INF/proxy-config.xml` from the primary node to the system where you are running the administrative console.

    g. In the **Specify the path to the file.** field, select **Local file system**.

    h. Click **Next** to proceed.

13. Run the generated Business Space DLL files to create Business Space database artifacts. You can find them in *wp_profile*/dbscripts/BusinessSpace directory where they were generated. Review the generated DDL files before running the scripts. Because the cluster shares a common database, these files must

only be run once. Use the `configBusinessSpaceDB.bat` or `configBusinessSpaceDB.sh` script for your database, depending on your platform. For more information about running the database scripts, see Configuring Business Space database tables.

14. To set up your BPM widgets on WebSphere Portal, run the installBusinessSpaceWidgetsOnPortal and updateEndpointBindingsOnPortal commands on the primary node. The widgets for the product are located in the *WebSphere_Portal_application_server*/BusinessSpace/widgets/*product_directory*.

  a. Type the following command:

    Jython example: `AdminTask.installBusinessSpaceWidgetsOnPortal ('[-clusterName `*WebSphere_Portal_cluster_name*` -dmHost `*deployment_manager_host_name*` -dmPort `*deployment_manager_SOAP_port*` -dmUser `*deployment_manager_user_ID*` -dmPassword `*deployment_manager_password*` -widgets /opt/IBM/WebSphere/AppServer/ BusinessSpace/widgets/WBM -portalusername `*user_name*` -portalpassword `*password*`]')`

    Jacl example: `$AdminTask installBusinessSpaceWidgetsOnPortal {-clusterName `*WebSphere_Portal_cluster_name*` -dmHost `*deployment_manager_host_name*` -dmPort `*deployment_manager_SOAP_port*` -dmUser `*deployment_manager_user_ID*` -dmPassword `*deployment_manager_password*` -widgets /opt/IBM/WebSphere/AppServer/ BusinessSpace/widgets/WBM -portalusername `*user_name*` -portalpassword `*password*`}`

  b. Update the endpoints files for your product widgets, available at *WebSphere_Portal_application_server*/BusinessSpace/registryData/ endpoints. For more information about your product-specific endpoints files, see Enabling Business Space widgets to work with multiple endpoints.

  c. Type the following command:

    Jython example: `AdminTask.updateEndpointBindingsOnPortal('[- clusterName `*WebSphere_Portal_cluster_name*` -dmHost `*deployment_manager_host_name*` -dmPort `*deployment_manager_SOAP_port*` -dmUser `*deployment_manager_user_ID*` -dmPassword `*deployment_manager_password*`]')`

    Jacl example: `$AdminTask updateEndpointBindingsOnPortal {-clusterName `*WebSphere_Portal_cluster_name*` -dmHost `*deployment_manager_host_name*` -dmPort `*deployment_manager_SOAP_port*` -dmUser `*deployment_manager_user_ID*` -dmPassword `*deployment_manager_password*`}`

15. Complete Business Space configuration on the deployment manager.

  a. Stop the deployment manager server.

  b. Install the V7.0.0.2 fix pack for your product on the deployment manager.

  c. Copy the BPM product widget EAR files from the primary node to *WebSphere_Portal_application_server*/installableApps/BusinessSpace/ on the deployment manager. BPM product widget EAR files are located in the widget compressed files in the *wp_profile*/BusinessSpace/widgets/ installw.*month-date-timestamp*/*widget_name*.widgets/ear directory, for example: C:/IBM/WebSphere/wp_profile/BusinessSpace/widgets/ installw.Jan-18-15.17.54-EST-2010/Dashboard.widgets/ear. Depending on the BPM products that you have installed, you might have multiple widgets installed.

Note: If you are using a Web server configured for your WebSphere Portal server, make sure to associate the newly installed applications to your Web server, regenerate the Web server plug-in, and restart the Web server. For more information about working with Web servers and Business Space, see Configuring a proxy server or load balancer to use with Business Space.

d. Start the deployment manager.

e. Connect to the deployment manager using wsadmin from `deployment_manager_profile_root`/bin.

For example, on Linus or UNIX, type: `./wsadmin.sh -conntype SOAP -host` `host_name` `-port` `SOAP PORT`-user `deployment_manager_user_name` `-password` `deployment_manager_password`.

f. Run the configureBusinessSpaceOnDMgr command. Use the same properties file that you used on primary node (or a copy). Do not change the file.

Jython example: `AdminTask.configureBusinessSpaceOnDMgr` `('[-dmgrServerName` `deployment_manager` `-dmgrNodeName` `deployment_manager_node` `-inputParamsFile /tmp/` `bscfg_linux.properties]')`

Jacl example: `$AdminTask configureBusinessSpaceOnDMgr {-dmgrServerName` `deployment_manager` `-dmgrNodeName` `deployment_manager_node` `-inputParamsFile /tmp/bscfg_linux.properties}`

Note: Logs might show errors similar to this one: `[4/2/10 23:24:22:429 EDT]` `00000030 ModuleManifes E?? UTLS0002E: The shared library WPSlib` `contains a classpath entry which does not resolve to a valid jar file,` `the library jar file is expected to be found at /opt/IBM/WebSphere/` `PortalServer/base/wp.ai.api/script/shared/app/scripting/` `wp.ai.api.script.jar`. These errors are a known limitation of a WebSphere Application Server Network Deployment environment and can be ignored.

16. If you are configuring additional BPM product widgets on top of your existing Business Space environment on WebSphere Portal, for each group of additional widgets, repeat steps 1 and 14. Then locate the BPM product widget EAR files in the widget compressed files in the `wp_profile/` `BusinessSpace/widgets/installw`.`month-date-timestamp/` `widget_name`.`widgets/ear`, install the EAR files using the administrative console, and associate the Web modules to the WebSphere Portal cluster.

17. Restart the WebSphere Portal servers on all nodes.

What to do next

After you have configured Business Space for WebSphere Portal, you must complete the following tasks to get the Business Space environment in WebSphere Portal ready for your business users:

• Configure single sign-on (SSO) and the Secure Sockets Layer (SSL) certificates for your widgets. For more information, see Configuring SSO and SSL for widgets on WebSphere Portal.

• Create a space on WebSphere Portal for your widgets. For more information, see Creating a space on WebSphere Portal for your Business Space widgets.

Note: Business Space uses a proxy component to connect to your REST services. In some cases if REST services are not responsive, you must update the connection timeout settings from Business Space to your REST service, depending on the performance of the REST service servers. If the REST service connections are

timing out, update the following settings. By default, the socket-timeout value is set to 10 seconds. Change it to an appropriate value for your situation. If you are using WebSphere Process Server administration widgets, set the initial timeout value to 30 seconds.

1. Open the file *wp_profile*/installedApps/*node_name*/AJAX Proxy Configuration.ear/wp.proxy.config.war/WEB-INF/proxy-config.xml

2. Change the `proxy:value` for `socket-timeout`. The time is specified in milliseconds.

   ```
   <proxy:meta-data>
    <proxy:name>socket-timeout</proxy:name>
    <proxy:value>10000</proxy:value>
   </proxy:meta-data>
   ```

3. Log in to the administrative console for WebSphere Portal.

4. Restart the AJAX Proxy Configuration application.

Example properties files for configuring Business Space on WebSphere Portal

Example properties files for configuring WebSphere Portal allow you to define parameters for your configuration. These examples are for a DB2 database.

Example properties file a server environment

```
############################################################################
#Example input parameter file for configureBusinessSpaceOnPortal
############################################################################
# There are two ways to invoke the command configureBusinessSpaceOnPortal.

#1. For a quick configuration using Derby embedded database and Business Space
# default values,
# use the following command.
# wsadmin>$AdminTask configureBusinessSpaceOnPortal { -serverName
# <WebSphere_Portal> -nodeName <NODE_NAME> -portalusername <admin>
# -portalpassword <admin> }
#2. Custom/detailed configuration by using this properties file.
#
# The command installBusinessSpaceOnPortal must be run
# before configureBusinessSpaceOnPortal is attempted.
# wsadmin>$AdminTask configureBusinessSpaceOnPortal { -serverName
# <WebSphere_Portal> -nodeName <NODE_NAME> -inputParamsFile
# <PATH_TO_bspaceconfig.properties> }
#
#
#
#config command inputs

serverName=WebSphere_Portal
nodeName=CONFI

#dbName defaults to BSPACE if nothing is specified
dbName=MYDBNAME

#schemaName defaults to IBMBUSSP if nothing is specified
schemaName=MYSCHEMA

# storageGroup defaults to BSPACE
storageGroup=

# Supported values for RDBMS include DB2, Oracle, SQLServer and DerbyEmbedded
RDBMS=DB2
dbserver=localhost
dbport=50000
dbusername=administrator
```

```
dbpassword=mypassword
driverPath=c:/IBM/SQLLIB/java
dbDirectoryDerbyEmbedded=

#specifies a directory path or file name prefix for the files used as the
# physical locations of table spaces. The default value is BSP.
# if tablespaceDir is not specified, tableSpaceName is used.
tablespaceNamePrefix=

#Instrumented= SQL output directory - leave value empty to use default for
#Business Space
outputDir=
#for Theme registration - used in ConfigEngine command.
portalusername=admin
portalpassword=admin
prodDirName=BusinessSpace


dmHost=
dmPort=
dmUser=
dmPassword=
#cluster - if you specify a cluster name, do not provide serverName or nodeName.
clusterName=
##########################################################################
```

Example properties file for a clustered environment

```
##########################################################################
#Example input parameter file for configureBusinessSpaceOnPortal
##########################################################################

#config command inputs

dbName=BSPACE
schemaName=BSPACE
##tableSpaceName=
storageGroup=
# Supported values for RDBMS include DB2, Oracle, and SQLServer
RDBMS=DB2
dbserver=localhost
dbport=50000
dbusername=db2user
dbpassword=password
driverPath=c:/IBM/SQLLIB/java
dbDirectoryDerbyEmbedded=
outputDir=
# The following are required for Theme registration - used in ConfigEngine command.
PortalAdminPwd=admin
WasPassword=password
prodDirName=BusinessSpace


dmHost=dmgr.mydomain.com
dmPort=8879
dmUser=admin
dmPassword=password
# If you specify a cluster name, do not provide serverName or nodeName.
clusterName=PortalCluster
portalusername=admin
portalpassword=password
##########################################################################
```

Configuring SSO and SSL for widgets on WebSphere Portal

If you want Business Space to work in WebSphere Portal, you must set up single
sign-on (SSO) with WebSphere Portal and your Business Space server and to make

sure the Secure Sockets Layer (SSL) certificates are exchanged between the servers for WebSphere Portal and Business Space.

About this task

If WebSphere Portal and your business process management product reside in separate cells, you must configure single sign-on between the two servers.

Your product offers Representational State Transfer (REST) APIs that can be accessed through the REST gateway. By default, the REST gateway is configured to accept only HTTPS connections. Because some widgets access these REST APIs, WebSphere Portal requires the SSL certificate imported from your product.

For the servers for both WebSphere Portal and your product, you must use the same user name and password to log on to the administrative console.

Procedure

1. Set up single sign-on with the WebSphere Portal server. For a clustered environment, complete this step on the administrative console of the deployment manager.
   a. Log on to the WebSphere Portal administrative console for the `WebSphere_Portal` server.
   b. Navigate to one of the following, depending on the version of WebSphere Application Server that you using with WebSphere Portal:
      - If you are using WebSphere Application Server V6.2, click **Security → Secure administration, applications and infrastructure** and then click **Authentication Mechanism and Expiration**.
      - If you are using WebSphere Application Server V7.0, click **Security → Global security** and then click **LTPA**.
   c. In the **Cross-cell single sign-on** section, type a password (this is only for encryption of the key file) and an absolute path for a key file.
   d. Click **Export keys**. The key file is generated.

   For a clustered environment, make sure to select **Synchronize changes with Nodes** on the Console Preferences page. (Navigate to **System administration → Console Preferences**.)
2. Set up single sign-on with the Business Space server. For a clustered environment, complete this step on the administrative console of the deployment manager.
   a. Log on to the administrative console of your business process management product.
   b. Navigate to **Security → Global security** and then click **LTPA**.
   c. In the **Cross-cell single sign-on** section, enter the password from step 1.c. and the absolute path to the key file.
   d. Click **Import keys**.
   e. Restart the Business Space server.

   For a clustered environment, make sure to select **Synchronize changes with Nodes** on the Console Preferences page. After single sign-on is configured, you can delete the key file.
3. Set up the Secure Sockets Layer (SSL) certificates so that they are exchanged between the WebSphere Portal and Business Space servers.
   a. Log on to the administrative console of WebSphere Portal.

b. Navigate to **Security → SSL certificates and key management**

c. Under Related Items, click **SSL configuration** and select **NodeDefaultSSLSettings**.

d. Under Related Items, click **Key stores and certificates** and select **NodeDefaultTrustStore**.

   If you use z/OS keyrings instead of the NodeDefaultTrustStore, see the related information "Importing a signer certificate from a truststore to a z/OS keyring."

e. Under Additional Properties, click **Signer Certificates**.

f. Make sure that your product server is running, click **Retrieve from Port**, and enter the correct host name and the HTTPS port of the `default_host` (default is 9443) in the two fields. You can select your own alias.

g. Click **Retrieve signer information**. WebSphere Portal loads the certificate and displays its information. If the certificate is not loaded, check the connection properties.

h. Click **OK** and save the configuration.

Creating a space on WebSphere Portal for your Business Space widgets

You begin working with Business Space widgets in WebSphere Portal by creating a space.

Procedure

1. Log on to WebSphere Portal.
2. Click **Business Space**.
3. Click **Manage Spaces**.
4. Create a space, using a template for your product widgets, and a Business Space theme.
   a. Click **Create Space**.
   b. Select a template that contains widgets provided with your business process management product.
   c. Select the **Business Space Theme** theme.
   d. Click **Save**.

Moving spaces to Business Space on WebSphere Portal

If you worked in the Business Space environment before deciding to use Business Space on WebSphere Portal, you can move spaces from the Business Space environment into WebSphere Portal.

Before you begin

Before you complete this task, you must have configured Business Space for WebSphere Portal.

You must be a Business Space administrator to perform the following steps.

Procedure

1. Log in to the Business Space environment where you created spaces (not in WebSphere Portal), and create a template from the space that you want to move into WebSphere Portal.

a. Click **Manage Spaces**. The Space Manager opens.

b. Next to the space you want to move, click **Actions** ▸ **Save as Template**.

2. Export that template.

   a. Click **Actions** ▸ **Manage Templates**.

   b. Next to the template that you created, click **Actions** ▸ **Export** and save the compressed file.

3. Log on to Business Space on WebSphere Portal and click **Business Space**.

   a. Click **Actions** ▸ **Manage Templates**.

   b. Click **Import Template** and select the compressed file that you exported from Business Space.

4. Create a space from that new template that you imported.

   a. Click **Manage Spaces**.

   b. Click **Create Space** and select the template that you imported.

5. If needed, change the owner of the space that you created to the original owner.

   a. Click **Manage Spaces**. The Space Manager opens.

   b. Next to the space, click **Actions** ▸ **Edit Settings** and change the Space owner.

   c.

6. If needed, the owner of the space can modify the settings for sharing the space.

   a. Click **Manage Spaces**. The Space Manager opens.

   b. Next to the space, click **Actions** ▸ **Share** and select the user IDs to grant access for viewing and editing the space.

7. Optional: Optionally, delete the templates that you created in Business Space and in Business Space on WebSphere Portal.

Migrating V6.2.x Business Space widgets to a V7.0 environment on WebSphere Portal

If you used Business Space widgets from a V6.2 product in WebSphere Portal, you can migrate them to work with your V7.0 environment in WebSphere Portal.

Before you begin

Before you complete this task, you must complete the following steps.

1. Upgrade your product (WebSphere Business Modeler Publishing Server V6.2.0.1, WebSphere Process Server V6.2.0.1, WebSphere ESB V6.2.0.1, or the WebSphere Process Server V6.2 and WebSphere Enterprise Service Bus V6.2 Feature Pack) to V7.

2. Upgrade WebSphere Portal V6.1.0.1 to WebSphere Portal V6.1.5.

3. Configure Business Space on WebSphere Portal and configure the necessary widgets for your V7.0 product (WebSphere Business Compass, WebSphere Process Server, or WebSphere Enterprise Service Bus). See Configuring Business Space on WebSphere Portal.

Procedure

1. Update the following properties in the `migrateIWidgets.properties` file for your environment. Migration scripts are located in `WebSphere_Application_Server_install_root`\BusinessSpace\scripts\portal\ `migration` on the WebSphere Portal server node.

```
Portal.Home=C:/IBM/WebSphere/Portal/PortalServer
Portal.userid=admin
Portal.password=admin
Portal.Url=http://localhost:10040
Portal.SOAP.Port=10033
```

2. Run the migration script `migrateIWidgets`. Migration scripts are located in *WebSphere_Application_Server_install_root*\BusinessSpace\scripts\portal\ migration.

    Run the appropriate migrateIWidgets script:

    - **On Linux and UNIX platforms:** `migrateIWidgets.sh –w` *WebSphere_Application_Server_install_root*
    - **On Windows platforms:** `migrateIWidgets.bat –w` *WebSphere_Application_Server_install_root*

What to do next

1. Log on to WebSphere Portal, click **Business Space**, and check that the pages for the migrated widgets appear properly.

    All the migrated pages are grouped into one default space: Business Space V7 Portal Migration Space.

2. Manually delete the pages that were configured with the old version of the widgets.

3. Manually delete the portlet instances for the old version of the widgets.

Commands (wsadmin scripting) for configuring Business Space on WebSphere Portal

Look up a scripting object or command class to find details about its command syntax.

To open the information center table of contents to the location of this reference information, click the **Show in Table of Contents** button ( ) on your information center border.

configureBusinessSpaceOnPortal command

Use the configureBusinessSpaceOnPortal command to configure the data source for Business Space and runs the scripts that configure the database tables.

This command configures the data source for Business Space on WebSphere Portal and prepares the scripts that configure the database tables.

Required parameters

-serverName *server_name*
> A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *node_name*
> A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-clusterName *cluster_name*
> A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

-dbName *database_name*
    A parameter that specifies the database for the configuration.

-inputParamsFile *properties_file_path*
    A parameter that specifies the path to the properties file that you are using to configure Business Space on WebSphere Portal. A properties file allows you to define parameters for your configuration. This parameter is required for configuring in a clustered environment and is optional for configuring on a server. For configuring on a cluster, if you are using a properties file, the only parameter you must specify is **-inputParamsFile**. If you are configuring on a server, if you specify this parameter, the only other parameters that are required are **-serverName** and **-nodeName**.

-portalusername *user_name*
    A parameter that specifies the WebSphere Portal administration user ID. If you want a default Business Space page and theme for Business Space on WebSphere Portal, specify both the **portalusername** and **portalpassword** parameters.

-portalpassword *password*
    A parameter that specifies the password for the WebSphere Portal administration user ID. If you want a default Business Space page and theme for Business Space on WebSphere Portal, specify both the **portalusername** and **portalpassword** parameters.

Optional parameters

-schemaName *schema_name*
    An optional parameter that specifies the database schema for the Business Space database configuration. The default value is IBMBUSSP.

-tablespaceDir *table_space_path*
    An optional parameter that specifies a directory path or file name prefix for the files used as the physical locations of table spaces. The default value is BSP. Valid for DB2, Oracle and SQL Server (otherwise ignored). For SQL Server, this parameter applies to the primary data file and log files.

-tablespaceNamePrefix *table_space_prefix*
    An optional parameter that specifies a prefix string added to the beginning of table space names to make them unique. The default value is BSP. If a table space name prefix is longer than four characters, it is truncated to four characters. Valid for DB2, DB2 z/OS V8, DB2 z/OS V9, and Oracle (otherwise ignored).

-storageGroup *storage_group*
    An optional parameter that specifies the storage group on z/OS for Business Space. If you are using z/OS, you must update the database scripts that are generated before running them. For more information about the scripts, see "Configuring Business Space database tables."

Examples

The following example uses configureBusinessSpaceOnPortal to configure a Business Space data source on a WebSphere Portal server.

- Jython example:

```
AdminTask.configureBusinessSpaceOnPortal('[-serverName
WebSphere_Portal_server -nodeName
WebSphere_Portal_node -inputParamsFile
/tmp/bspace/bscfg_linux.properties]')
```

- Jacl example:

```
$AdminTask configureBusinessSpaceOnPortal {-serverName
 WebSphere_Portal_server -nodeName
WebSphere_Portal_node -inputParamsFile
 /tmp/bspace/bscfg_linux.properties}
```

installBusinessSpaceOnPortal command

Use the installBusinessSpaceOnPortal command to set up Business Space powered by WebSphere on your WebSphere Portal runtime environment.

The installBusinessSpaceOnPortal command installs Business Space on your WebSphere Portal runtime environment.

Required parameters

-serverName *server_name*
> A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *node_name*
> A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-user *user_ID*
> A parameter that specifies the user ID for the server. For configuring Business Space on a server, you must specify a **user**.

-password *password*
> A parameter that specifies the password for the server. For configuring Business Space on a server, you must specify a **password**.

-clusterName *cluster_name*
> A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

-dmHost *deployment_manager_host_name*
> A parameter that specifies the name of the deployment manager host. For configuring Business Space on a cluster, you must specify a **dmHost**.

-dmPort *deployment_manager_SOAP_port*
> A parameter that specifies the SOAP port name. For configuring Business Space on a cluster, you must specify a **dmPort**.

-dmUser *deployment_manager_user_ID*
> A parameter that specifies the user ID for the deployment manager. For configuring Business Space on a cluster, you must specify a **dmUser**.

-dmPassword *deployment_manager_password*
> A parameter that specifies the password for the deployment manager. For configuring Business Space on a cluster, you must specify a **dmPassword**.

-portalRoot *path_to_Portal_Server*
> A parameter that specifies the path where WebSphere Portal Server is installed.

Examples

The following example uses installBusinessSpaceOnPortal to install Business Space on WebSphere Portal Server for a server configuration.

- Jython example:

```
    AdminTask.installBusinessSpaceOnPortal('[-serverName WebSphere_Portal
     -nodeName myNode -user admin -password admin
    -portalRoot C:\IBM\WebSphere\PortalServer]')
```

- Jacl example:

```
    $AdminTask installBusinessSpaceOnPortal {-serverName WebSphere_Portal
     -nodeName myNode -user admin -password admin
    -portalRoot C:\IBM\WebSphere\PortalServer}
```

The following example uses installBusinessSpaceOnPortal to install Business Space
on WebSphere Portal Server for a cluster configuration.

- Jython example:

```
    AdminTask.installBusinessSpaceOnPortal('[-clusterName PortalCluster
     -dmHost dmgr.domain.com -dmPort 8879 -dmUser admin -dmPassword admin
    -portalRoot C:\IBM\WebSphere\PortalServer]')
```

- Jacl example:

```
    $AdminTask installBusinessSpaceOnPortal {-clusterName PortalCluster
     -dmHost dmgr.domain.com -dmPort 8879 -dmUser admin -dmPassword admin
    -portalRoot C:\IBM\WebSphere\PortalServer}
```

installBusinessSpaceWidgetsOnPortal command

Use the installBusinessSpaceWidgetsOnPortal command to install, deploy and
register widgets for use with Business Space on WebSphere Portal.

The installBusinessSpaceWidgetsOnPortal command installs, deploys, and registers
designated widgets contained in a compressed file or an enterprise archive (EAR)
file. If widgets are already deployed, the installBusinessSpaceWidgetsOnPortal
command refreshes the binary and registration information. Before you run this
command, edit the *wp_profile*\ConfigEngine\properties\wkplc.properties file,
and set the value for WasPassword to the administrative password for the
WebSphere Application Server that you are using with WebSphere Portal, and the
value for PortalAdminPwd to the administrative password for your WebSphere
Portal product.

Required parameters

-serverName *WebSphere_Portal_server_name*
    A parameter that specifies the server name for the configuration. For
    configuring Business Space on a server, you must specify both a **serverName**
    and a **nodeName**.

-nodeName *WebSphere_Portal_node_name*
    A parameter that specifies the node name for the configuration. Either a
    serverName, nodeName, or clusterName is required. For configuring Business
    Space widgets on a server, you must specify both a **serverName** and a
    nodeName.

-clusterName *WebSphere_Portal_cluster_name*
    A parameter that specifies the cluster name for the configuration. For
    configuring Business Space widgets on a cluster, you must specify a
    clusterName.

-dmHost *deployment_manager_host_name*
    A parameter that specifies the name of the deployment manager host. For
    configuring Business Space on a cluster, you must specify a **dmHost**.

-dmPort *deployment_manager_SOAP_port*
    A parameter that specifies the SOAP port name. For configuring Business
    Space on a cluster, you must specify a **dmPort**.

-dmUser *deployment_manager_user_ID*
A parameter that specifies the user ID for the deployment manager. For configuring Business Space on a cluster, you must specify a **dmUser**.

-dmPassword *deployment_manager_password*
A parameter that specifies the password for the deployment manager. For configuring Business Space on a cluster, you must specify a **dmPassword**.

-widgets *widgets_path*
A parameter that specifies one of the following:
- the full path for the directory that contains the compressed files or the EAR files that contain the widgets. If you specify a directory, all widgets will be installed for all compressed files and EAR files in that directory.
- the full path to an individual compressed file that contains the widgets.
- the full path to an individual EAR file that contains the widgets.

-portalusername *user_name*
A parameter that specifies the WebSphere Portal administration user ID. This parameter is required for template registration. Specify this parameter if your widget has templates.

-portalpassword *password*
A parameter that specifies the password for the WebSphere Portal administration user ID. This parameter is required for template registration. Specify this parameter if your widget has templates. This parameter must be specified if the **portalusername** parameter is specified.

Optional parameters

–noEndpoints true|false
Specifies that you do not want to update the specified endpoint files that are contained in the widgets compressed file.

Examples

The following example uses installBusinessSpaceWidgetsOnPortal to install, deploy, and register widgets on a WebSphere Portal server. It specifies a compressed file that contains the widgets.

- Jython example:

```
AdminTask.installBusinessSpaceWidgetsOnPortal('[-nodeName
WebSphere_Portal_node_name -serverName
 WebSphere_Portal_server_name -widgets
 install_root\BusinessSpace\widgets\MyWidget.zip
  -portalusername user_name -portalpassword
 password]')
```

- Jacl example:

```
$AdminTask installBusinessSpaceWidgetsOnPortal {-nodeName
WebSphere_Portal_node_name -serverName
 WebSphere_Portal_server_name -widgets
 install_root\BusinessSpace\widgets\MyWidget.zip
 -portalusername user_name -portalpassword
 password}
```

The following example uses installBusinessSpaceWidgetsOnPortal to install, deploy, and register widgets on a WebSphere Portal cluster. It specifies the path to a directory where widgets are located.

- Jython example:

```
AdminTask.installBusinessSpaceWidgetsOnPortal ('[-clusterName
WebSphere_Portal_cluster_name -dmHost deployment_manager_host_name
-dmPort deployment_manager_SOAP_port -dmUser
deployment_manager_user_ID -dmPassword deployment_manager_password
-widgets install_root\BusinessSpace\widgets\MyWidget.zip -portalusername
user_name -portalpassword password]')
```
- Jacl example:

```
$AdminTask installBusinessSpaceWidgetsOnPortal {-clusterName
WebSphere_Portal_cluster_name -dmHost deployment_manager_host_name
-dmPort deployment_manager_SOAP_port -dmUser
deployment_manager_user_ID -dmPassword deployment_manager_password
-widgets install_root\BusinessSpace\widgets\MyWidget.zip -portalusername
user_name -portalpassword password}
```

updateEndpointBindingsOnPortal command

Use the updateEndpointBindingsOnPortal command to register configured and enabled Representational State Transfer (REST) endpoints so that your team can use the widgets in Business Space on WebSphere Portal.

This command registers the configured REST service endpoints so that Business Space is properly connected to widgets for your product. This command can only be used to register the endpoints of the REST services that are in the same cell as Business Space. For a clustered environment, make sure to run the command from wsadmin scripting on the deployment manager.

Before you run this command, you must update the endpoints files for your product widgets. For a server, the endpoints files are available at *WebSphere_Portal_application_server*/BusinessSpace/registryData/endpoints. For a clustered environment, the endpoints files are available at *deployment_manager_application_server*/BusinessSpace/registryData/endpoints. For more information about your product-specific endpoints files, see Enabling Business Space widgets to work with multiple endpoints.

Required parameters

-serverName *WebSphere_Portal_server_name*
    A parameter that specifies the server name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-nodeName *WebSphere_Portal_node_name*
    A parameter that specifies the node name for the configuration. For configuring Business Space on a server, you must specify both a **serverName** and a **nodeName**.

-clusterName *WebSphere_Portal_cluster_name*
    A parameter that specifies the cluster name for the configuration. For configuring Business Space on a cluster, you must specify a **clusterName**.

-dmHost *deployment_manager_host_name*
    A parameter that specifies the name of the deployment manager host. For configuring Business Space on a cluster, you must specify a **dmHost**.

-dmPort *deployment_manager_SOAP_port*
    A parameter that specifies the SOAP port name. For configuring Business Space on a cluster, you must specify a **dmPort**.

-dmUser *deployment_manager_user_ID*
    A parameter that specifies the user ID for the deployment manager. For configuring Business Space on a cluster, you must specify a **dmUser**.

-dmPassword *deployment_manager_password*
> A parameter that specifies the password for the deployment manager. For configuring Business Space on a cluster, you must specify a **dmPassword**.

Examples

The following example registers all configured and enabled REST services on the WebSphere Portal server with Business Space.

- Jython example:

```
AdminTask.updateEndpointBindingsOnPortal('[-serverName
WebSphere_Portal_server_name
 -nodeName WebSphere_Portal_node]')
```

- Jacl example:

```
$AdminTask updateEndpointBindingsOnPortal {-serverName
WebSphere_Portal_server_name
 -nodeName WebSphere_Portal_node}
```

The following example registers all configured and enabled REST services on the WebSphere Portal cluster with Business Space.

- Jython example:

```
AdminTask.updateEndpointBindingsOnPortal('[-clusterName
 WebSphere_Portal_cluster_name -dmHost
 deployment_manager_host_name -dmPort
 deployment_manager_SOAP_port -dmUser
 deployment_manager_user_ID -dmPassword
 deployment_manager_password]')
```

- Jacl example:

```
$AdminTask updateEndpointBindingsOnPortal {-clusterName
 WebSphere_Portal_cluster_name -dmHost
 deployment_manager_host_name -dmPort
 deployment_manager_SOAP_port -dmUser
 deployment_manager_user_ID -dmPassword
 deployment_manager_password}
```

Configuring business rules and selectors

Business rules and selectors provide flexibility in a business process by changing the results of a process based on a criteria. Before installing applications that contain business rules and selector components, you must install the business rules dynamic repository. You can install the business rules dynamic repository for a stand-alone server or for network deployment.

Configuring the business rule and selector audit log

You can configure the server to use different values than the default values for the log that keeps track of new, changed, and deleted business rules and selectors. Changing the configuration can help you conserve resources on your server.

Before you begin

You must be at the administrative console to perform this task.

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as a configurator to perform this task.

About this task

After you have run your server in production for a while, you may have determined that the default values the server uses for the business rules and selectors audit log need adjustment.

To configure the business rule and selector audit log, perform the following steps.

Procedure

1. Navigate to the **Business Rules and Selectors Auditing** page by clicking **Servers > Application servers >** *servername* **Business Rules > Business Rules and Selectors Auditing**.

2. Do one of the following depending on the type of change you want.

Type of change	Actions
Immediate	1. Select the **Runtime** tab. 2. Enter the desired changes. 3. **Optional:** To make the changes permanent, copy them to the repository by selecting **Save runtime changes to configuration as well**. 4. Click **OK** to make the changes and return to the previous page or **Apply** to make the changes and remain on this page.
Delayed	1. Select the **Configuration** tab. 2. Enter the desired changes. 3. Click **OK** to make the changes and return to the previous page or **Apply** to make the changes and remain on this page. 4. When you want the changes to take effect, restart the server.

Results

The audit log takes the attributes you specified.

Note: You may need to modify the configuration for business rules and selector auditing due to the way the server user identity is specified when security is enabled with WebSphere Application Server 6.1. If the default value is used for the server user identity, an automatically generated server identity value is recorded in the audit record for the user when any auditable action involving business rules or selectors is performed when the application containing the business rules or selectors is started after business rule or selector installation. An auditable action occurs when a business rule or selector artifact is changed through application startup after install, management clients, or import or export through the administrative console. The generated value may not match the format of other user IDs used in other audit records, and you may want a more consistent value.

You can specify a server identity by selecting the option to use a "Server identity that is stored in the repository," which will associate a user ID that is in the user repository with the server process. The audit records will use this identity when

auditable actions involving business rules or selectors are performed when the application containing the business rules or selectors is started after the business rule or selector artifacts are installed in the repository.

The server identity value has no effect on audit actions involving changes through management clients such as the business rules manager or other administrative actions such as exporting or importing business rule groups. For these actions, the audit record will use the authenticated user.

For more information on changing the server user identity, see the topics under Securing applications and their environment and the WebSphere Application Server WebSphere Application Server Network Deployment Security documentation.

Configuring business rule and selector auditing using commands

Use commands to configure business rule and selector auditing when you need to change any of the characteristics while a server is running.

Before you begin

You must run these commands from a command line environment for the server.

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as a configurator to perform this task.

About this task

There may be occasions when you need to change how many servers audit business rules and selectors and cannot restart the servers involved. Using the command line, you can automate configuring the servers in a batch mode. The following tasks show how to use commands to configure one server.

Important: These settings are not saved if you restart the server. To save the configuration after entering these commands, you must use the administrative console. Select **Servers > Server Types > WebSphere application servers >** *servername* **> Business Rules > Business Rules and Selectors Auditing > Runtime** or **Servers > Server Types > WebSphere application servers >** *servername* **> Selectors > Business Rules and Selector Auditing > Runtime**.

To configure business rule and selector auditing using commands, perform the following steps.

Note: The following task configures server `server1`. If the server is not named server1, replace `server1` below with the name of the server. All of the steps beginning at step 3 could be placed in a jacl script and run that way.

Procedure

1. Enter the administrative environment.

    `wsadmin`

2. Decide whether you are configuring audit logging or changing an existing configuration.

Task	Command
Configuring audit logging	`set mbean [$AdminControl queryNames` `*:*,name=CustomizationAuditMBean,process=server1]`
Changing audit logging configuration	`set auditconfig [$AdminConfig list AuditLog]`

3. Enter the appropriate commands.

Commands to configure or change audit logging

Important: When entering commands that change an existing configuration, you must save the changes. The changes do not take effect until you restart the server.

The following are the commands you can enter:

$AdminControl invoke $mbean getSeparateAuditLogEnabled
> Use to determine whether logging is occurring to a separate audit log.

$AdminControl invoke $mbean setSystemOutAuditLogEnabled {*boolean*}
> Use to enable or disable logging to the `SystemOut.log` file. *Boolean* can either be true or false.

$AdminControl invoke $mbean getSeparateAuditLogFileName
> Use to determine the file name of the separate audit log.

$AdminControl invoke $mbean setSeparateAuditLogFileName {*filename*}
> Use to set the name of the new log file, for example, `MyAudit.log`.

$AdminControl invoke $mbean getSeparateAuditLogFileRolloverSize
> Use to determine the size of the audit log.

$AdminControl invoke $mbean setSeparateAuditLogFileRolloverSize *integer*
> Use to set the size of the audit log before the system rolls it over into a history file. The size is in megabytes.

$AdminControl invoke $mbean getSeparateAuditLogFileMaxNumberOfBackupFiles
> Use to determine the number of audit log history files.

$AdminControl invoke setSeparateAuditLogFileMaxNumberOfBackupFiles *integer* Use to set the number of audit log history files.

$AdminControl invoke $mbean setSeparateAuditLogEnabled {*boolean*}
> Use to start or stop logging to a separate log file. *Boolean* can either be true or false.

$AdminConfig showall $auditconfig
> Use to show the current audit log configuration.

$AdminConfig modify $auditconfig {{separateAuditLogEnabled true}}
> Use to enable logging to a separate audit log.

$AdminConfig modify $auditconfig {{systemOutAuditLogEnabled false}}
> Use to disable auditing to the `system.Out` file.

$AdminConfig modify $auditconfig {{customAuditLog {{maxNumberOfBackupFiles 7} {rolloverSize 7}}}}
> Use to change the number of audit log history files and the size of the audit log file.

$AdminConfig modify $auditconfig {{customAuditLog {{fileName MyAudit.log}}}}
> Use to change the name of the audit log file.

$AdminConfig save
> Use to save the configuration.

What to do next

Save these changes by opening the administrative console and selecting **Servers > Server Types > WebSphere application servers >** *servername* **> Business Rules > Business Rules and Selectors Auditing > Runtime** or **Servers > Server Types > WebSphere application servers >** *servername* **> Selectors > Business Rules and Selector Auditing > Runtime**. Alternatively, enter $AdminConfig save.

Note: You may need to modify the configuration for business rules and selector auditing due to the way the server user identity is specified when security is enabled with WebSphere Application Server 6.1. If the default value is used for the server user identity, an automatically generated server identity value is recorded in the audit record for the user when any auditable action involving business rules or selectors is performed when the application containing the business rules or selectors is started after business rule or selector installation. An auditable action occurs when a business rule or selector artifact is changed through application startup after install, management clients, or import or export through the administrative console. The generated value may not match the format of other user IDs used in other audit records, and you may want a more consistent value.

You can specify a server identity by selecting the option to use a "Server identity that is stored in the repository," which will associate a user ID that is in the user repository with the server process. The audit records will use this identity when auditable actions involving business rules or selectors are performed when the application containing the business rules or selectors is started after the business rule or selector artifacts are installed in the repository.

The server identity value has no effect on audit actions involving changes through management clients such as the business rules manager or other administrative actions such as exporting or importing business rule groups. For these actions, the audit record will use the authenticated user.

For more information on changing the server user identity, see the topics under Securing applications and their environment and the WebSphere Application Server WebSphere Application Server Network Deployment Security documentation.

Considerations for installing the business rules manager

If you are planning to use the business rules manager in a distributed environment, you must understand the concepts of cells, nodes, and clusters and how to set up the business rules manager for best performance during run time.

The application server is organized on the concept of cells, nodes and servers. In a stand-alone server configuration, a cell contains one node, and each node contains one server. System administration applications and user applications all run in the same server. In a stand-alone server configuration, you can install the business rules manager in the same application server, and it can be accessed by the default URL.

In a distributed server configuration, you can configure a cell to contain multiple nodes, and each node can contain multiple application servers. Each cell constitutes a single administrative domain. With this configuration, you can use central administration, workload management, and failover configuration for the entire domain.

For best performance in a distributed server configuration, install the business rules manager on the administrative deployment target, an application server in the cell where business administration services are centrally hosted. This server is typically the same server that hosts the Common Event Infrastructure service.

Within a cell, all servers use and share a single business rules repository. When you access the business rules repository, you can access all dynamic business rule artifact definitions regardless of the exact location where the business application is installed.

Because of this central storage for all business rules in the cell at run time, you can deploy the business rules manager to any application servers in the cell, and the business rules manager gives a consistent view of all business rules within the cell. However, because of high-availability considerations, it is recommended that system administrators deploy the business rules manager into the administrative deployment target, a dedicated application server in the cell where business administration services are centrally hosted. The administrative deployment target server is the same server where the Common Event Infrastructure service and other business administrative applications are installed. With this configuration, when you require high availability, you can cluster the administrative deployment target server to provide a scalable solution to the application users.

Installing the business rules manager using the administrative console

You can install the business rules manager as an enterprise application on WebSphere Process Server to manage business rules during run time. For WebSphere Process Server 6.1 and higher, you can install the business rules manager simultaneously when creating a WebSphere Process Server profile by selecting the check box on the Business Rules Manager Configuration page of the Profile Management tool. Alternatively, you can install the business rules manager using three other methods: through the configuration page of the administrative console, by using the JACL command for your operating system, or by using the Admin Tasks command (this method is for WebSphere Process Server 6.1 and higher). For more information, see the individual topics for each installation method.

Before you begin

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as an administrator or a configurator to perform this task.

About this task

To install the business rules manager using the administrative console, perform the following steps.

Procedure
1. Ensure that the administrative console is running.

2. In the navigation pane click **Servers > Server Types > WebSphere application servers** or **Servers > Clusters > WebSphere application server clusters**.

3. Select the name of your server or cluster target.

4. On the Configuration-tabbed page, under **Business Integration**, expand **Business Rules** and click **Business Rules Manager Configuration**.

5. Under **General Properties** select the **Install business rules manager** check box.

   Note: If the business rules manager has already been installed, the check box will be checked but grayed out as it is not possible to uninstall the business rules manager from this page. However, you can uninstall it manually by going to the list of applications and uninstalling it from there.

6. In the **Context root** field either accept the default context root of /br or type a custom context root for the business rules manager URL.

7. Click **OK**.

8. Save the configuration.

What to do next

In the navigation pane click **Applications > Application Types > WebSphere enterprise applications** and select **Start Business Rules Manager**.

Installing the business rules manager using the JACL command

You can use a JACL command for Windows, Linux, i5/OS, as an alternative to using the administrative console for installing the business rules manager. Using a JACL command is possible if you did not already install the business rules manager when you installed WebSphere Process Server and created profiles.

Before you begin

Required security role for this task: When security and role-based authorization are enabled, you must be authenticated with a user ID that has been assigned to the administrator or configurator role to perform this task.

About this task

To install the business rules manager using the JACL command, perform the following steps.

Procedure

1. Ensure that WebSphere Process Server is started.

2. Open the shell environment or command prompt for your operating system, and go to the *install_root*/bin directory (*install_root*\bin directory for Windows).

3. Run the specific installation command for your operating system, as follows:

   - For Windows, run: wsadmin.bat -f installBRManager.jacl [-s *servername* -n *nodename* | -cl *clustername*] -ce *cellname* -r *rootname*

   - For Linux, run: wsadmin.sh -f ./installBRManager.jacl [-s *servername* -n *nodename* | -cl *clustername*] -ce *cellname* -r *rootname*

   - For i5/OS, run: wsadmin -f ./installBRManager.jacl [-s *servername* -n *nodename* | -cl *clustername*] -ce *cellname* -r *rootname*

   To install and map the business rules manager to more than one target, run the following command for your operating system:

- For Windows, run: wsadmin.bat -f installBRManager.jacl -m "{{target1} {target2} ... {targetn}}" -ce *cellname* -r *rootname*
- For Linux, run: wsadmin.sh -f installBRManager.jacl -m "{{target1} {target2} ... {targetn}}" -ce *cellname* -r *rootname*
- For i5/OS, run: wsadmin -f installBRManager.jacl -m "{{target1} {target2} ... {targetn}}" -ce *cellname* -r *rootname*
- For z/OS, run: wsadmin.sh -f installBRManager.jacl -m "{{target1} {target2} ... {targetn}}" -ce *cellname* -r *rootname*

Note: The parameter "-m" (implying "multiple") allows you to install and map the business rules manager to many targets at the same time. A pair of double quotation marks encloses the targets.

where:

servername
> The name of the application server.
>
> The pair of arguments "-s servername" is required in the Network Deployment configuration if a cluster is not specified. If missing, the default value of *servername* is "server1".

nodename
> The name of the installation node.
>
> The pair of arguments "-n nodename" is required in the Network Deployment configuration if a cluster is not specified.

clustername
> The name of the cluster where you want to install the application.
>
> The pair of arguments "-cl clustername" is required in the Network Deployment configuration if a server name and a node name are not specified.
>
> **Note:** You must either specify the node and server or specify the cluster. Do not specify both.

cellname
> The name of the installation cell.
>
> The pair of arguments "-ce cellname" is optional.

rootname
> The name of the application root directory.
>
> The pair of arguments "-r rootname" is optional. If missing, the default value of *rootname* is "/br".

target*i* The target (where *i* is 1, 2, ..., n) to which you want to install and map the business rules manager.
> The target can be either (-s *servername* and -n *nodename*) or -cl *clustername*.

Important: If WebSphere Process Server is configured in a single-server environment, all of these pairs of arguments are optional. If WebSphere Process Server is configured for a Network Deployment environment, one of the following argument pairs is required:
- either (-s *servername* and -n *nodename*)
- or -cl *clustername*

- or -m "{{target1} {target2} ... {targetn}}"

The other argument pairs are optional.

Example

Example: Suppose that you want to map the business rules manager application to the following targets:

- cluster "BofACluster"
- Web server "RedirectorServer" and node "AIXNode01"
- application server "LinuxServer" and node "LinuxNode02"

on context root "bofa/brm"

You would run the command, as follows:

```
install_root/bin/wsadmin -f installBRManager.jacl -m "{{-cl BofACluster}
{-n AIXNode01 -s RedirectorServer} {-s LinuxServer -n LinuxNode02}}" -r
bofa/brm
```

Installing the business rules manager using the AdminTask command

With WebSphere Process Server 6.1 and higher, you can install the business rules manager using the Admin Task command. Similar to using the administrative console or the JACL command, use the Admin Task command if you did not install the business rules manager when you installed WebSphere Process Server and created profiles.

Before you begin

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as an administrator or a configurator to perform this task.

About this task

To install the business rules manager using the admin task command, perform the following steps.

Procedure

1. Ensure that WebSphere Process Server is started.
2. In a command window, go the WebSphere Process Server home directory and change to the directory /bin.
3. Run the wsadmin command to enter the wsadmin mode.
4. Enter one of the following commands to install the business rules manager:

   wsadmin> $AdminTask configBusinessRulesManager {-*serverName* <serverName>
   -*nodeName* <nodeName> -*contextRoot* <contextRoot>}

   Or

   wsadmin> $AdminTask configBusinessRulesManager {-*clusterName*
   <clusterName> -*contextRoot* <contextRoot>}

   where

   serverName
          The name of the application server.

> *nodeName*
>> The name of the installation node.
>
> *clusterName*
>> The name of the cluster where you want to install the application.
>
> *contextRoot*
>> The context root used to launch the application. The default value is /br.

5. Run `wsadmin> $AdminConfig save` to save the configuration.

   Tip: You can run `$AdminTask help configBusinessRulesManager` to learn more about its parameters.

Example

Example: To install the business rules manager on server "cvuServer" and node "cvuNode01" with context root "br", you should enter the following command:

```
wsadmin> $AdminTask configBusinessRulesManager {-serverName cvuServer
-nodeName cvuNode01 -contextRoot br}
```

Then to save the configuration, enter:

```
wsadmin> $AdminConfig save
```

Configuring server security for the business rules manager

If you want to use security with your server, you must configure the server that is using the business rules manager. On a server where security is not enabled, you can use the business rules manager without additional configuration.

About this task

If you have different roles or user IDs, you must set administrative security when configuring your server. To set security for your server, perform the following steps.

Procedure

1. Set administrative security on user IDs by assigning a role to each ID when creating the user IDs. Create each user ID and map each user ID to the role `BusinessRuleUser`.

   To set the role, navigate to the business rule manager application (**Applications > Enterprise Applications**), select the business rule manager application, select the Security role to user/group mapping and update the BusinessRuleUser role.

   In addition to the BusinessRuleUser role, two other roles are defined: NoOne and AnyOne. NoOne is be used by developers to explicitly set the resources that should not be accessed directly. AnyOne is used by Tivoli Access Manager to obtain authorization for a WebSphere Process Server environment.

   Note: In an ND environment with administrative security turned on, if you plan to run the business rules manager on port 908n, where n is a positive integer, you should make sure that port "944(n+3)" with the host value of "*" was configured. If there is no such port, manually configure it before you launch the business rules manager.

2. Set the session tracking mechanism to use cookies to track sessions.

3. At a minimum, set an appropriate session timeout value.

Configuring a Web browser for the business rules manager

The server configures a client automatically while installing the business rules manager, but you must ensure that the Web browser is configured correctly for the business rules manager to work properly.

About this task

To ensure that the Web browser is configured correctly for the business rules manager, perform the following steps.

Procedure

1. Make sure that scripting is enabled in the Web browser.

   The business rules manager requires scripting to function.

2. Make sure that cookies are enabled.

   When necessary, cookies are used to track the session when you are using the business rules manager. Therefore, enable cookies on your browser when tracking sessions. Contact your system administrator if you enable cookies.

Configuring the relationship service

After installing the product, you need to set the configuration properties for the relationship service.

Before you begin

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as a configurator or an administrator to perform this task. Any WebSphere security role can view this configuration.

About this task

To set the data source and query block size (relationship instance count) properties for the relationship service, perform the following steps.

Procedure

1. Ensure that the administrative console is running.
2. In the navigation pane, click **Integration Applications > Relationship Manager.**
3. Click **Relationship Services configuration**.

   The configuration tabbed page displays, showing the name and version (read-only) of the currently installed relationship service.

4. In the **Query block size (relationship instance count)** field, specify the maximum cache that the relationship service should set aside for relationship queries. This setting determines the size of the query results set. By default, 5000 relationship instances are read at once. This field controls the server size memory usage and provides the administrator with a level of control over how much memory resource is consumable by any given query.

5. In the **Data source** field, specify the default data source for the relationship service by entering the Java Naming and Directory Interface (JNDI) name of a data source defined at the cell level. This is where the tables for the relationship service are stored. Each relationship-related schema is created in this data source by default.

6. You then have the following options:

   - Click **OK** to save your changes and return to the previous page.

- Click **Reset** to clear your changes and restore the currently configured values or most recently saved values.
- Click **Cancel** to discard any unsaved changes on the page and return to the previous page.

Configuring extended messaging resources

Use the administrative console to configure resources needed by the extended messaging service and the applications that use the service. You can enable the extended messaging service, configure listener port extensions to handle late responses, and add or modify input and output ports for applications that use extended messaging.

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

Extended messaging enables container-managed messaging. It extends the base Java Message Service (JMS) support, the Enterprise Java Bean (EJB) component model, and support for EJB 2.0 message-driven beans to allow use of the existing container-managed persistence and transactional behavior.

Extended messaging uses the bean-managed messaging implementation to provide the JMS interfaces, which ensures that both bean-managed and extended messaging use consistent JMS support. JMS usage is simplified since its support is managed by the extended messaging service.

For a complete description of extended messaging, see the following articles in the WebSphere Business Integration Server Foundation information center:

- Extended messaging: Overview
- Using extended messaging in applications

Enabling the Extended Messaging Service

Enable the Extended Messaging Service to provide runtime support for container-managed messaging (extended messaging). Use the Extended Messaging Service page to specify whether this service starts automatically when the application server starts or whether it must be started manually.

About this task

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

Required security role for this task: When security and role-based authorization are enabled, you must log in as an administrator or configurator to perform this task.

To enable the Extended Messaging Service, perform the following steps.

Procedure

1. Ensure that the administrative console is running.
2. Click **Servers** → **Server Types** → **WebSphere application servers** → *server_name* → **Extended Messaging Service** to display the Extended Messaging Service page.
3. If you want to enable the Extended Messaging Service to start automatically with server startup, select the **Enable service at server startup** check box. If you want to start the service manually, ensure the check box is cleared.
4. Click **OK**.
5. When prompted, click **Save** on the console task bar to save your changes to the master repository.
6. If you are using the WebSphere MQSeries bindings transport in your configuration, set the value of the MQ_INSTALL_ROOT environment variable as follows:
   a. From within the administrative console, click **Environment** → **WebSphere Variables**.
   b. Click MQ_INSTALL_ROOT to display the configuration page for the environment variable.
   c. In the **Value** field, delete the default value (`${WAS_INSTALL_ROOT}/lib/WMQ`) and replace it with the explicit installation path (for example, `D:/IBM/WebSphereMQ` on a Windows system).
   d. Click **OK**.
7. Stop and restart the application server in order for the changes to take effect.

Configuring listener port extensions to handle late responses

To enable a listener port to handle late responses, configure an extension that specifies how often the port checks for responses and how long it waits for those responses.

About this task

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

Late responses occur when the messaging infrastructure delays a response to a message sent by a sender bean, thereby preventing the application from receiving that response. Extended messaging can retrieve these late response messages and pass them to a message-driven bean provided by the application to handle late responses.

Required security role for this task: When security and role-based authorization are enabled, you must log in as an administrator or configurator to perform this task.

To create and enable a listener port extension that handles late responses, perform the following steps.

Procedure

1. Ensure you have a listener port defined and configured, and that you have deployed the sender bean with the **Handle late responses** option enabled.

   Note: For more information about deploying a sender bean with this option enabled, refer to the WebSphere Business Integration Server Foundation Information Center.

2. From the administrative console, click **Servers** → **Server Types** → **WebSphere application servers** → *server_name* → **Extended Messaging Service** → **Listener Port Extensions** .

3. From the Listener Port Extensions page, click **New** to create a new listener port extension.

4. From the New Listener Port Extension page, select the **Enabled** check box to enable the extension and late response handling.

5. In the **Request Interval** field, either accept the default value or specify a new value to indicate how often the listener port checks for late responses.

6. In the **Request Timeout** field, either accept the default value or specify a new value to indicate how long the listener port waits for a late response. The listener port discards any responses received after the specified timeout value.

7. Use the **Listener Ports** drop-down menu to specify the listener port to use for the extension.

8. Click **OK**.

9. When prompted, click **Save** on the console task bar to save your changes to the master repository.

10. Stop and restart the application server in order for the changes to take effect.

What to do next

After you create a listener port extension, you can modify its configuration as necessary by using the Listener Port Extensions settings page.

Selecting extended messaging providers

Select the extended messaging provider you want to administer by clicking the appropriate scope on the Extended Messaging Provider page. Each scope (cell, node, and server) that contains applications that use extended messaging has its own extended messaging provider to manage resources. You can create, modify or delete input ports, output ports, or other custom properties for each provider.

About this task

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as administrator, operator, configurator, or monitor to perform this task.

To select the extended messaging provider you want to administer, perform the following steps.

Procedure

1. From the administrative console, click **Resources > Extended Messaging Provider**.
2. From the Extended Messaging Provider page, select the appropriate scope for the extended messaging provider you want to administer.
   - **Cell**: The most general scope. Extended messaging resources defined at the cell scope are visible from all nodes and servers, unless they have been overridden.
   - **Node**: Extended messaging resources defined at the node scope override any duplicates defined at the cell scope. They are visible to all servers on the same node, unless they have been overridden at a server scope on that node.
   - **Server**: Extended messaging resources defined at the server scope override any duplicate definitions defined at the cell or parent node scope. They are visible only to a specific server.

   For detailed information about scopes, see the WebSphere Application Server Information Center.
3. Click **Apply**.

Results

The administrative console updates the **Scope**, **Name**, and **Description** fields on the bottom of the page to reflect the values for the selected resource provider.

What to do next

You can now create, modify or delete input ports, output ports, or other custom properties for the selected extended messaging provider.

Configuring input ports

Use the administrative console to create new or modify existing input ports for each receiver bean that is constructed from a session bean. Input ports define properties for the receiving Java Message Service (JMS) destination, specify how to select and handle messages, and provide details for any required reply destinations.

About this task

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

You do not need to create input ports for receiver beans that are constructed from message-driven beans; the necessary details are associated with the deployed message-driven bean and the Message Listener Service.

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as administrator or configurator to perform this task.

To add or modify an input port, perform the following steps.

Procedure

1. From the administrative console, click **Resources > Extended Messaging Provider**.
2. From the Extended Messaging Provider page, select the appropriate scope for the resource provider you want to work with.
3. Click **Apply**.
4. Click **Input Ports** from the Additional Properties table.
5. From the Input Port collection page, do one of the following:
   - If you are creating a new input port, click **New**.
   - If you want to modify an existing input port, click the port name.
6. From the Input Port settings page, specify the appropriate properties for the input port.
7. Click **OK**.
8. When prompted, click **Save** on the console task bar to save your changes to the master repository.
9. Stop and restart the application server in order for the changes to take effect.

Input port settings:

When you create a new input port or modify an existing input port, you must specify certain properties. Use the information in this topic to determine whether a property is optional or required and what data type it accepts.

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

An input port has the following configuration properties:

Scope The scope at which the extended messaging provider is defined. The value represents the location of the configuration file. The administrative console automatically populates this field. You cannot edit the value.

Name The name of the input port, used for administrative purposes. This field requires a string value.

JNDI Name
The Java Naming and Directory Interface (JNDI) name for the input port. This field requires a string value.

Description
A description of the input port, used for administrative purposes. This field is optional, and it accepts a string value.

Category
A category string to use when classifying or grouping the resource. This field is optional, and it accepts a string with a maximum of 30 ASCII characters.

JMS Connection Factory JNDI Name
The JNDI name for the Java Message Service (JMS) connection factory used by the input port. This field requires a string value (for example, `jms/connFactory1`).

JMS Destination JNDI Name

The JNDI name for the JMS destination used by the input port. This field requires a string value (for example, `jms/destn1`).

JMS Acknowledgement Mode

The JMS mode that is used to acknowledge messages. This field is required for message-driven beans that use bean-managed transaction demarcation (in other words, the transaction type is set to `Bean`).

The following are valid values for this field:

- Auto Acknowledge: The session automatically acknowledges a message in either of the following cases:
  - When the session successfully returns from a call to receive a message
  - When the session calls a message listener to process the message and receives a successful response from that listener
- Dups OK Acknowledge: The session acknowledges only the delivery of messages. This can result in the delivery of duplicate messages if JMS fails.

The default mode is Auto Acknowledge.

Destination Type

The JMS resource type. This field requires one of the following values: :

- Queue: The receiver bean receives messages from a queue destination.
- Topic: The receiver bean receives messages from a topic destination.

The default value is Queue.

Subscription Durability

Specifies whether a JMS topic subscription is durable. This field is required if the JMS destination type is a topic. The following are valid values for this field:

- Durable: A subscriber registers a durable subscription with a unique identity that is retained by JMS. Subsequent subscriber objects with the same identity resume the subscription in the state in which it was left by the previous subscriber. If there is no active subscriber for a durable subscription, JMS retains the subscription's messages until they are received or they expire.
- NonDurable: Nondurable subscriptions last for the lifetime of their subscriber. A client sees the messages published on a topic only while its subscriber is active. If the subscriber is inactive, the client misses the messages published on its topic.

The default value is NonDurable.

Reply JMS Connection Factory JNDI Name

The JNDI name of the JMS connection factory that is used for replies. This field requires a string value (for example, `jms/connFactory1`).

Reply JMS Destination JNDI Name

The JNDI name of the JMS destination that is used for replies. This field requires a string value (for example, `jms/destn1`).

Configuring output ports

Use the administrative console to create new or modify existing output ports for sender beans. Output ports specify the properties sender beans need to define the destinations for sent messages. They also specify optional properties when responses are expected. Output ports are associated with sender beans at deployment time.

About this task

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

Required security role for this task: When security and role-based authorization are enabled, you must be logged in as administrator or configurator to perform this task.

To add or modify an output port, perform the following steps.

Procedure

1. From the administrative console, click **Resources > Extended Messaging Provider**.
2. From the Extended Messaging Provider page, select the appropriate scope for the extended messaging provider you want to modify.
3. Click **Apply**.
4. Click **Output Ports** from the Additional Properties table.
5. From the Output Port collection page, do one of the following:
   - If you want to add a new output port, click **New**.
   - If you want to modify an existing output port, click the port name.
6. From the Output Port settings page, specify the appropriate properties for the output port.
7. Click **OK**.
8. When prompted, click **Save** on the console task bar to save your changes to the master repository.
9. Stop and restart the application server in order for the changes to take effect.

Output port settings:

When you create a new output port or modify an existing output port, you must specify certain properties. Use the information in this topic to determine whether a property is optional or required and what data type it accepts.

Important: The Extended Messaging Service feature was deprecated in WebSphere Process Server 6.0.x and is no longer available for application use as of WebSphere Process Server 6.2, except when managing any 6.0.x nodes that exist in a cell during migration. Replace any existing applications which depend on Extended Messaging services with ones that use standard JMS APIs, or equivalent messaging technologies.

An output port has the following configuration properties:

Scope The extended messaging provider scope; the value represents the location of the configuration file. The administrative console automatically populates this field. You cannot edit the value.

Name The name of the output port, used for administrative purposes. This field requires a string value.

JNDI Name

The Java Naming and Directory Interface (JNDI) name for the output port. This field requires a string value.

Description

A description of the output port, used for administrative purposes. This field is optional, and it accepts a string value.

Category

A category string to use when classifying or grouping the resource. This field is optional. It accepts a string value with a maximum of 30 ASCII characters.

JMS Connection Factory JNDI Name

The JNDI name for the Java Message Service (JMS) connection factory used by the output port. This field requires a string value (for example, `jms/connFactory1`).

JMS Destination JNDI Name

The JNDI name for the JMS destination used by the output port. This field requires a string value (for example, `jms/destn1`).

JMS Delivery Mode

The JMS mode used to deliver messages. You must select one of the following values for this field:

- Persistent: Messages put onto the destination are persistent.
- Nonpersistent: Messages put onto the destination are not persistent.

The default value is Persistent.

JMS Priority

The message priority for the queue destination. This field requires an integer value from 0 to 9. The default value is 4.

JMS Time To Live

The time, in milliseconds, a message remains in the queue. After the specified time elapses, the message expires.

This field requires an integer with a value from 0 to n:

- 0: Messages never time out.
- n: Messages time out after n milliseconds.

The default value is 0.

JMS Disable Message I.D.

Specifies whether the system generates a JMS message ID. This is a required field; select one of the following values:

- Selected: The system does not generate JMS message IDs.
- Cleared: The system generates JMS message IDs automatically.

By default, JMS message IDs are generated.

JMS Disabled Message Timestamp

Specifies whether the system generates a JMS message timestamp. This is a required field; select one of the following values:

- Selected: The system does not add message timestamps to sent messages.
- Cleared: The system automatically adds message timestamps to sent messages.

By default, the system adds message timestamps to sent messages.

Response JMS Connection Factory JNDI Name
The JNDI name of the JMS connection factory that is used for responses handled by the output port. This field requires a string value (for example, `jms/connFactory1`).

Response JMS Destination JNDI Name
The JNDI name of the JMS destination that is used for responses handled by the output port. This field requires a string value (for example, `jms/destn1`).

Setting up the messaging server environment

Before running any XMS applications, including the sample applications provided with XMS, you must set up the messaging server environment.

About this task

The steps that you need to complete to set up the messaging server environment depend on the artifacts that an application connects to, and whether you are using the Message Service Client for .NET or the Message Service Client for C/C++. The steps are described in the documentation for the type of client.

Procedure
- Setting up for Message Service Client for .NET
- Setting up for Message Service Client for C/C++

What to do next

You can use the sample applications provided with the Message Service clients to verify your installation and messaging server setup. For more information about using the sample applications, see the following topics:
- Using .NET sample XMS applications
- Using C/C++ sample XMS applications

Configuring the JNDILookup Web Service

If you are using the administered JMS objects provided by WebSphere Process Server with Message Service Clients for C/C++ and .NET, you must configure the JNDILookup Web Service that WebSphere Process Server provides to enable non-Java clients to access administered JMS objects from a non-Java environment.

Before you begin

Before starting this task, make sure that the JNDILookup Web Service application has been installed.

About this task

Administratively defined ConnectionFactory and Destination objects provide a separation between a JMS implementation and the JMS interfaces, which makes JMS client applications more portable since they are sheltered from the implementation details of a JMS provider. Administered objects enable an administrator to manage the connection settings for client applications from a

central repository. For example, the specific queue that an application uses can be altered by changing the administered Destination object that the application obtains via JNDI.

Non-Java clients such as Message Service Clients for C/C++ and .NET can also use administered objects. However, since the administered JMS objects provided by WebSphere Process Server are serialized Java objects accessed via JNDI, non-Java clients are not able to interpret them properly without the use of the JNDILookup Web Service. This web service provides a lookup operation that allows Message Service Clients for C/C++ and .NET to request the retrieval of a JNDI object by specifying the name of the object. The properties of the administered object are returned to the application using a Map of name/value pairs.

Procedure

Define the JNDILookup Web Service URL within the Message Service Client for C/C++ or Message Service Client for .NET application. To define the web service URL within an application, set the XMSC_IC_URL property of the InitialContext object to the web service endpoint URL. This property can alternatively be specified as an argument on constructing the InitialContext object.

Configuring Common Event Infrastructure

You can configure Common Event Infrastructure resources, or change existing resources, using the server AdminTask object

About this task

Common Event Infrastructure (CEI) can be installed with a default configuration that is fully functional on a stand-alone server configuration. You would only perform this configuration to create a stand-alone server profile using the Profile Management Tool. In all other cases, you use the administrative console to configure CEI — such as when you are installing it in a network deployment environment or in a cluster — to ensure that the configuration is appropriate on your system.

You can also use the wsadmin command to configure CEI, or you can use the command to alter an existing CEI configuration. In either case, you would change the configuration of CEI by using the server AdminTask object to run administrative commands.

After changing CEI configuration, you must restart the server or cluster.

Common Event Infrastructure components

Common Event Infrastructure components are installed as a set of applications, services, and resources on the server.

When you configure Common Event Infrastructure, a number of components are created and deployed on your server.

Common Event Infrastructure service
  A service installed into the server, that enables applications and clients to use Common Event Infrastructure. You can view the configuration of the Common Event Infrastructure service in the administrative console, as follows:

- For a server, select **Servers > Application Servers >** *server_name* **> Business Integration > Common Event Infrastructure > Common Event Infrastructure Service**.

- For a cluster, select **Servers > Clusters >** *cluster_name* **> Business Integration > Common Event Infrastructure > Common Event Infrastructure Service**.

If the check box labeled "Enable the event infrastructure server" is selected, then the service is installed and running or it will start after you restart your server or cluster. If it is cleared, then the service is not installed or will be uninstalled after you restart your server or cluster

Event service settings
A set of properties used by the event service that enable event distribution and persistence using the data store. Typically, no configuration is necessary for this resource, but you might need to create additional event service settings if you want to set up multiple event services in the same cell. To view the event service settings, click **Service integration > Event service > Event service settings**.

Event messaging configuration
The resources that support asynchronous event transmission to the event service using the Java Messaging Service (JMS). The default messaging configuration uses the server embedded messaging. You can optionally configure an external JMS provider for event messaging.

Event database
The event database is used to persistently store events received by the event service. The Derby database is included as part of the server, but is not recommended for use in production environments. Instead, you can configure an external event database on the following products: DB2, Oracle, SQLServer, and Informix.

Event filter plug-in
A filter plug-in is used to filter events at the source using XPath event selectors. To configure the filter properties, click **Service Integration > Common Event Infrastructure > Event Emitter Factories > Event Filter Settings**.

Emitter factory
An emitter factory is an object used by event sources to create emitters; an emitter is used to send events to the event service. The properties of an emitter factory affect the behavior of any emitter that is created using that emitter factory. To view the available emitter factories, click **Service Integration > Common Event Infrastructure > Event Emitter Factories**.

Event service transmission
An event service transmission is an object defining properties that determine how emitters access the event service synchronously using EJB calls; these properties are used by emitter factories when creating new emitters. You can view or change the available event service transmissions from the emitter factory settings.

JMS transmission
A JMS transmission is an object that defines properties that determine how emitters access the event service asynchronously using a JMS queue; these properties are used by emitter factories when creating new emitters. You can view or change the available JMS transmissions from the emitter factory settings.

Event group

An event group is a logical collection of events used to categorize events according to their content. When querying events from the event service or subscribing to event distribution, an event consumer can specify an event group to retrieve only the events in that group. Event groups can also be used to specify which events should be stored in the persistent data store. To view the available event groups in the administrative console, click **Service integration > Common Event Infrastructure > Event service > Event services >** *event_service* **> Event groups**.

Configuring the Common Event Infrastructure using the administrative console

ConfigureCommon Event Infrastructure by using the server administrative console.

About this task

Open the Common Event Infrastructure Server panel of administrative console:

If you are configuring a server, select **Servers > Server Types > WebSphere application servers >** *server_name* **> Business Integration > Common Event Infrastructure > Common Event Infrastructure Server**.

If you are configuring a cluster, click **Servers > Clusters > WebSphere application server clusters >** *cluster_name* **> Business Integration > Common Event Infrastructure > Common Event Infrastructure Server**.

Procedure

1. Enable the deployment of the Common Event Infrastructure enterprise application by selecting the check box labeled **Enable the event infrastructure server**. If the server has already been configured, then you can enable or disable it by selecting or clearing the check box. If the enable check box is cleared then Common Event Infrastructure has not been configured, or has had a previous configuration disabled but the server has not been restarted. An information message shows you whether this deployment target has Common Event Infrastructure configured. If the server has already been configured, you can change the data source settings for the event database, the message store, or both.

   Note: If you select the check box to enable the Common Event Infrastructure server and the server has not yet been configured, then the parameters shown is used to configure it unless you change them.

   - If you are performing the configuration the first time, then the event data source tables are created on the common database. If there is already a Common Event Infrastructure server configuration, then you need to create a database.
   - The messaging service is created under a unique schema under the common database.

   When the server/cluster on which Common Event Infrastructure has been configured is restarted, then the new changes take effect.

2. Configure (or change the current settings for an existing configuration of) the event database by using one of the following methods to populate the fields with the appropriate settings.

   - Click **Edit** for a database configuration panel with a more extensive list of options than the ones listed on the panel.

- Use the fields on the panel to enter the information:
  a. **Database name** – the name of the database you use to store events.
  b. **Create Tables** – select this check box if you want to create the database tables on the event database.

     Note: If you are configuring Common Event Infrastructure to use a database on another server, then you are not be able to create the tables using this control. Instead, you will have to use the database scripts that will be generated after you complete the rest of this configuration. In this case, you can click **Edit** to show the data source detail panel, which tells you the location of the database creation scripts.
  c. **Username** and **Password** – for authenticating into the event database.
  d. **Server** – name of the server where the event database is located.
  e. **Provider** – choose a provider for your database from the menu.

  Note: The **Schema** field is activated only if the database is created using DB2 on an iSeries or z/OS platform. In all other cases, the schema field is disabled.

  Important: If the tables exist on the target database, then the configuration can fail.
3. Select whether the Common Event Infrastructure bus is to be**Local** on the server, or **Remote** and reside on another server. If you choose remote, then select the remote location from the menu or click **New** to create a new remote bus.
4. Configure Common Event Infrastructure support for messaging.
   - Click Edit for a database configuration panel with a more extensive list of options than the ones listed on the panel.
   - Use the fields on the panel to enter the information:
   a. **Database name** – enter the name of the database you use to store messages.
   b. **Schema** – enter a name for the schema, or accept the default name given.
   c. **Username** and **Password** – for authenticating into the messaging database.
   d. **Server** – name of the server where the messaging database is located.
   e. **Provider** – choose a provider for your database from the menu.
5. Create a messaging authentication alias for the Common Event Infrastructure bus.
   a. Select **Additional Properties > JMS Authentication Alias**.
   b. Enter the user ID and password you use for secure communications across the System Integration Bus. You can accept the default configured values of "CEI" for both the user ID and password if security is disabled. If security has been enabled, then enter the user ID and password used for the bus authentication. In a production environment, you would select your own user ID and password to secure the system.
   c. Click **OK**.
6. Click **OK** or **Apply**.
7. Restart your server or cluster.

Results

All the major parts of Common Event Infrastructure are now configured and running on your server or cluster. The configuration includes the event data store, the messaging engine, and the event application. This single panel can be used in

place of many commands and steps you would otherwise use to configure Common Event Infrastructure.

What to do next

After you have restarted your server or cluster, you will be able to store service component events that are emitted from your applications. You can now change the runtime properties of the Common Event Infrastructure server by selecting the **Common Event Infrastructure Destination** panel. You can choose whether to start the Common Event Infrastructure server at startup, and specify the emitter factory JNDI name where the events are sent.

Deploying the Common Event Infrastructure application

Before you can use Common Event Infrastructure, you must first deploy the event service and associated resources in the server runtime environment.

About this task

The Common Event Infrastructure enterprise application includes the runtime components of the event service and the default messaging configuration used for asynchronous event submission.

To deploy the event service:

Procedure

From the wsadmin tool, run the **deployEventService** administrative command in batch or interactive mode. The parameters of the **deployEventService** administrative command are as follows:

nodeName
  The name of the node where the event service to be deployed. This parameter is optional; if you do not specify a node name, the default is the current node. If you specify a node name, then you must also specify the server name using the **serverName** parameter. This parameter is not valid if you are deploying the event service in a cluster.

serverName
  The name of the server where the event service to be deployed. This parameter is required only if you specify a node; it is not valid if you are deploying the event service in a cluster.

clusterName
  The name of the cluster where the event service to be deployed. This parameter is optional and must not be specified if you are deploying at the node or server scope.

enable
  Indicates whether the event service to be started automatically when the server starts. The default value is `true`.

Results

After the administrative command completes, the Common Event Infrastructure event service and default messaging configuration are deployed at the specified scope.

What to do next

If WebSphere security is enabled, you must also configure the JMS authentication alias and password using the **setEventServiceJmsAuthAlias** administrative command.

If you are deploying the event service in a cluster, you must also manually configure the event database.

Deploying Common Event Infrastructure in a cluster

There are several ways you can deploy Common Event Infrastructure resources in a cluster environment.

Deploying Common Event Infrastructure in an existing cluster:

You can deploy the event service application in an existing cluster.

About this task

Deploying the event service application in a cluster is essentially the same as deploying the application on a stand-alone server. However, in a cluster environment, no default event database is configured.

To deploy and configure Common Event Infrastructure in a cluster environment:

Procedure

1. Run the **deployEventService** administrative command as you would for a stand-alone server, but specifying the name of the cluster. Use the clusterName parameter to specify the cluster.
2. On the deployment manager system, run the database configuration administrative command. Specify the cluster name using the clusterName parameter. This command generates the database configuration script.
3. Copy the generated database configuration script to the database system.
4. Run the database configuration script on the database system to create the event database.
5. On the deployment manager system, run the **enableEventService** command to enable the event service. Use the clusterName parameter to specify the name of the cluster.

Creating a cluster by converting an existing Common Event Infrastructure server:

You can create a cluster by converting an existing stand-alone server that is already configured with Common Event Infrastructure.

Before you begin

Before you can convert the existing server, make sure that it is fully configured for Common Event Infrastructure. The configuration includes deploying the event service application and configuring the event database.

About this task

To create the cluster:

Procedure

1. Follow the typical WebSphere process for converting a stand-alone server into the first member of a new cluster. When the server is converted, the following steps take place:

    * Common Event Infrastructure resources available at the scope of the server are moved to the new cluster scope.

      Default database: If the existing server is configured with the default Derby database, the database resources are not moved to the cluster scope. Instead, these resources are removed. The default database configuration is not supported in a cluster. In this situation, the event service in the cluster is disabled by default.

    * The deployed event service application target list is modified to remove the converted server and add the new cluster.

2. Optional: If the converted server was configured with the default Derby database, you must configure a new event database for the cluster and then enable the event service:

    a. On the deployment manager system, run the database configuration administrative command. Specify the cluster name using the clusterName parameter. This command generates the database configuration script.

    b. Copy the generated database configuration script to the database system.

    c. Run the database configuration script on the database system to create the event database.

    d. On the deployment manager system, run the **enableEventService** command to enable the event service. Use the clusterName parameter to specify the name of the cluster.

Creating a cluster by using an existing Common Event Infrastructure server as a template:

You can create a cluster by specifying an existing Common Event Infrastructure server as a template.

Before you begin

Before you can create a cluster using this method, you must have an existing server that is fully configured for Common Event Infrastructure. The configuration includes deploying the event service application and configuring the event database.

About this task

To create the cluster:

Procedure

1. Follow the typical WebSphere process for creating new cluster, using the existing Common Event Infrastructure server as a template for the first cluster member. When the first member is created, the following steps take place:

    * Common Event Infrastructure resources available at the scope of the existing server are copied to the new cluster scope.

      Default database: If the existing server is configured with the default Derby database, the database resources are not copied to the cluster scope. The

default database configuration is not supported in a cluster. In this situation, the event service in the cluster is disabled by default.

- The deployed event service application target list is modified to include the new cluster.

2. Optional: If the existing server was configured with the default Derby database, you must configure a new event database for the cluster and then enable the event service:

   a. On the deployment manager system, run the database configuration administrative command. Specify the cluster name using the clusterName parameter. This command generates the database configuration script.

   b. Copy the generated database configuration script to the database system.

   c. Run the database configuration script on the database system to create the event database.

   d. On the deployment manager system, run the **enableEventService** command to enable the event service. Use the clusterName parameter to specify the name of the cluster.

Configuring event messaging

You can modify the messaging configuration used for JMS transmission of events to the event service.

About this task

You will create the messaging infrastructure for Common Event Infrastructure when you use the administrative console panel to configure Common Event Infrastructure on a server. Generally, the messaging configuration will use the default messaging provider and create a single JMS queue for asynchronous transmission of events to the event service. You can, if necessary, modify this messaging configuration.

Configuring additional JMS queues

If you are using the default event messaging configuration, you can add additional JMS queues for transmission of events to the event service.

About this task

To configure an additional JMS queues using the default messaging configuration, you can set up multiple JMS queues that are routed to the service integration bus queue destination. The Common Event Infrastructure service integration bus queue destination depends upon the scope at which the event service is deployed:

Scope	Service integration bus queue destination
Server	*node.server*.CommonEventInfrastructureQueueDestination
Cluster	*cluster*.CommonEventInfrastructureQueueDestination

For more information about service integration bus configuration, refer to the documentation.

Configuring event messaging using an external JMS provider

If you do not want to use the default embedded messaging configuration for event transmission, you can configure asynchronous message transport to use an external Java Messaging Service (JMS) provider.

Before you begin

Before you can configure event messaging using an external JMS provider, you must first create a JMS queue and connection factory using the appropriate interfaces for your JMS provider. You must also create a listener port or activation specification.

About this task

To configure event messaging using an external JMS provider:

Procedure

From the wsadmin tool, run the **deployEventServiceMdb** administrative command in batch or interactive mode. The parameters of the **deployEventServiceMdb** command are as follows:

applicationName
: The application name of the event service message-driven bean to be deployed. This parameter is required.

nodeName
: The name of the node where the event service message-driven bean is to be deployed. If you specify a node name, you must also specify a server name. The node name is an optional parameter; the default value is the current node. Do not specify this parameter if you are deploying the application in a cluster.

serverName
: The name of the server where the event service message-driven bean is to be deployed. This parameter is required if you are deploying the application at server scope; otherwise it is optional. Do not specify a server name if you are deploying the application in a cluster.

clusterName
: The name of the cluster where the event service message-driven bean is to be deployed. Specify this parameter only if you are deploying the application in a cluster.

listenerPort
: The name of the listener port used by the event service message-driven bean to publish events. The specified listener port must exist. You must specify either a listener port or an activation specification, but not both.

activationSpec
: The JNDI name of the activation specification used by the event service message-driven bean to publish events. The specified activation specification must exist. You must specify either a listener port or an activation specification, but not both.

qcfJndiName
: The JNDI name of the JMS queue connection factory to be used by the event service message-driven bean. This parameter is required if you specify an activation specification; otherwise it is optional. If you specify a queue connection factory and a listener port, the queue connection factory must match the one configured for the listener port.

Results

The **deployEventServiceMdb** administrative command deploys the message-driven bean for the event service, configured for the specified listener port or activation specification. It also creates an emitter factory and JMS transmission using the external JMS configuration. Applications can use either the default emitter factory (which is configured to use the default messaging configuration) or the new emitter factory (which uses the external JMS provider).

What to do next

If you want to set up more than one JMS queue to the event service, you can run this command multiple times, specifying different enterprise application names and JMS queues. Each time you run the script, it deploys an additional message-driven bean and configures new resources to use the specified JMS queue.

Configuring the JMS authentication alias

If WebSphere security is enabled and you want to use asynchronous JMS messaging to submit events to the event service, you must configure the JMS authentication alias.

About this task

To configure the JMS authentication alias:

Procedure

From the wsadmin tool, run the **setEventServiceJmsAuthAlias** administrative command in batch or interactive mode. The parameters of the **setEventServiceJmsAuthAlias** command are as follows:

userName
> The name of the user to be used for the JMS authentication alias. This parameter is required.

password
> The password of the user to be used for the JMS authentication alias. This parameter is required.

nodeName
> The name of the node where you want to update or create the JMS authentication alias. If you specify a node name, you must also specify a server name. Do not specify a node name if you are configuring the authentication alias in a cluster.

serverName
> The name of the server where you want to update or create the JMS authentication alias. This parameter is required only if you specify a node; it is not valid if you are configuring the authentication alias in a cluster.

clusterName
> The name of the cluster where you want to update or create the JMS authentication alias. Specify this parameter only if you are configuring the authentication alias in a cluster; if you specify a cluster name, do not specify a node or server name.

Results

The JMS authentication alias used by the event service objects is updated at the specified scope; if the authentication does not exist, it is created using the specified values.

Configuring the event database

You can configure the event data source using commands that are specific for each supported database product.

About this task

The event database is required to support persistence of events. If you did not use the Common Event Infrastructure configuration panel in the administrative console, you still have the option of creating the event database by using the commands described here.

Event database limitations

Some limitations apply to configurations of the event database using certain database software.

Refer to the following table to see which limitations might apply to your environment.

Table 188. Event database limitations

Database type	Limitations
Oracle	• The Oracle 11 JDBC thin driver imposes some size restrictions for string values if you are using a Unicode character set. You may receive an Oracle ORA-01461 error when events containing large values (such as a long message attribute) are stored in the event database. For more information about this restriction, refer to the Oracle 11 documentation. To avoid this problem, use the Oracle 11 OCI driver or the Oracle 11 thin driver. • Oracle database software treats a blank string as a NULL value. If you specify a blank string as an event attribute value, that string is converted to a NULL when it is stored in an Oracle event database.

Table 188. Event database limitations (continued)

Database type	Limitations
Informix	• The JDBC 3.0 driver (or later) is required. Previous versions of the JDBC driver do not provide full support for the required XA transactions. • The database configuration and removal scripts generated by the **configEventServiceInformixDB** administrative command require the **dbaccess** command in order to run SQL scripts. This command might be available only on the Informix server. Therefore, if the Informix server is on a different system from the WebSphere server, the database configuration scripts might need to be copied to the Informix server and run locally.
SQL Server	• The SQL Server database must be configured to use mixed authentication mode. Trusted connections are not supported. • The XA stored procedures must be installed. These stored procedures are provided with the JDBC driver from Microsoft Corporation. • The sqljdbc.dll file must be available in a directory specified on the PATH statement. This file is provided with the JDBC driver from Microsoft Corporation. • The Distributed Transaction Coordinator (DTC) service must be started.

Configuring a Derby event database

You can configure a Derby event database at the server or cluster scope on a Linux, UNIX, or Windows system.

About this task

There are two types of Derby databases that you can use for the event database: Derby embedded and Derby Network. Both types are shipped with WebSphere Application Server, but they have limited functionality that is not suitable for a production environment. Therefore, use Derby as the event database only for purposes such as development or testing. For more information about the Derby databases, see the WebSphere Application Server documentation (linked to at the bottom of this page).

Derby embedded can only be used with a stand-alone server. Consequently, if you ever federate your stand-alone server to a cluster or ND environment, then you need to completely reconfigure your event data source with another database product. It automatically starts when you start the server.

Derby Network can be used in a clustered or ND environment, although still be avoided in use with actual production systems. You need to manually start the database to use it with the server.

To configure a Derby event database:

Procedure

1. Start the wsadmin tool.
2. Use the AdminTask object to run the **configEventServiceDerbyDB** administrative command in batch or interactive mode. The minimum required parameters of the **configEventServerDerbyDB** command are as follows:

   createDB
   > Indicates whether the administrative command creates and run the database configuration scripts. Specify `true` or `false`. If this parameter is set to `false`, the scripts are created but are not run. You must then run the database configuration scripts to complete the database configuration.

   nodeName
   > The name of the node that contains the server where the event service data source is created. If you specify a node name, you must also specify a server name. You must specify one of the following:
   > - node name and server name
   > - cluster name

   serverName
   > The name of the server where the event service data source is created.

   clusterName
   > The name of the cluster where the event service data source is created. If you specify a cluster name, do not specify node and server names.

   Other parameters might be required for your environment. For a complete list of parameters and usage information, refer to the help for the **configEventServiceDerbyDB** administrative command.

Results

The administrative command creates the required data source at the specified scope; if you specified `true` for the createDB parameter, the command also runs the generated database configuration script to create the database.

The generated database configuration scripts are stored by default in the *profile_root*/databases/event/*node*/*server*/dbscripts/derby directory. (In a Network Deployment environment, these scripts are stored under the deployment manager profile directory.) If you specified a value for the optional outputScriptDir parameter, the scripts are stored in that location instead. You can use these scripts to manually configure the event database at any time.

Configuring a DB2 event database (Linux, UNIX, and Windows systems)

You can configure an external event database using DB2 Universal Database on a Linux, UNIX, or Windows system.

About this task

To configure a DB2 event database on a Linux, UNIX, or Windows system:

Procedure

1. Start the wsadmin tool.

2. Use the AdminTask object to run the **configEventServiceDB2DB** administrative command in batch or interactive mode. The minimum required parameters of the **configEventServiceDB2DB** command are as follows:

createDB
Indicates whether the administrative command creates and run the database configuration scripts. Specify `true` or `false`. If this parameter is set to `false`, the scripts are created but are not run. You must then run the database configuration scripts to complete the database configuration.

nodeName
The name of the node that contains the server where the event service data source is created. If you specify a node name, you must also specify a server name. You must specify one of the following:

- Node name and server name
- Cluster name

serverName
The name of the server where the event service data source is created.

clusterName
The name of the cluster where the event service data source is created. If you specify a cluster name, do not specify node and server names.

jdbcClassPath
The path to the JDBC driver. Specify only the path to the driver file; do not specify the file name.

dbHostName
The host name of the server where the database is installed.

dbUser
The DB2 user ID to use when creating the event database. The specified user ID must have sufficient privileges to create and drop databases.

dbPassword
The DB2 password to use.

Other parameters might be required for your environment. For a complete list of parameters and usage information, refer to the help for the **configEventServiceDB2DB** administrative command.

Results

The administrative command creates the required data source at the specified scope; if you specified `true` for the createDB parameter, the command also runs the generated database configuration script to create the database.

The generated database configuration scripts are stored by default in the *profile_root*/databases/event/*node*/*server*/dbscripts/db2 directory. (In a Network Deployment environment, these scripts are stored under the deployment manager profile directory.) If you specified a value for the optional outputScriptDir parameter, the scripts are stored in that location instead. You can use these scripts to manually configure the event database at any time.

Configuring a DB2 database on a z/OS system
You can configure an event database on a z/OS system using DB2 database software.

Before you begin

To configure the DB2 database from a remote client, you must have the DB2 Connect product installed with the latest fix packs.

About this task

To configure the event database:

Procedure

1. Linux   UNIX   Windows   If you are configuring the z/OS event database from a Linux, UNIX, or Windows client system, follow these steps to create and catalog the database:

   a. On the z/OS system, use the DB2 administration menu to create a subsystem.

   b. Optional: Create the storage group you want to use for the event database. You can also use an existing storage group (for example, `sysdeflt`).

   c. Enable the 4 K, 8 K, and 16 K buffer pools you want to use for the event database.

   d. Grant the necessary permissions to the user ID you want the data source to use. This user ID must have rights to access the database and storage group you created; it must also have permission to create new tables, table spaces, and indexes for the database.

   e. Catalog the remote database. Run the following commands, either in a script or in a DB2 command-line window:

   ```
   catalog tcpip node zosnode remote hostname server IP_port
       system db_subsystem
   catalog database db_name as db_name at node zosnode authentication DCS
   ```

   For more information about how to catalog a node and its databases, refer to the DB2 Connect documentation.

   f. Verify that you can establish a connection to the remote subsystem. You can run the following command to perform the verification:

   ```
   db2 connect to subsystem user userid using password
   ```

   g. Bind to the host database. Run the following commands:

   ```
   db2 connect to db_name user userid using password
   db2 bind db2_root/bnd/@ddcsmvs.lst blocking all sqlerror continue message
       mvs.msg grant public
   db2 connect reset
   ```

   For more information about binding a client to a host database, refer to the DB2 Connect documentation.

2. On the WebSphere system, start the wsadmin tool.

3. Use the AdminTask object to run the **configEventServiceDB2ZOSDB** administrative command in batch or interactive mode. The minimum required parameters of the **configEventServiceDB2ZOSDB** command are as follows:

   createDB

   Linux   UNIX   Windows   Indicates whether the administrative command creates and run the database configuration scripts. This parameter applies only if you are running the administrative command from a Linux, UNIX, or Windows client system. Specify `true` or `false`.

If this parameter is set to `false`, or if you are running the command on the z/OS system, the scripts are created but are not run. You must then run the database configuration scripts to complete the database configuration.

nodeName

The name of the node that contains the server where the event service data source is created. If you specify a node name, you must also specify a server name. You must specify one of the following:

- Node name and server name
- Cluster name

serverName

The name of the server where the event service data source is created.

clusterName

The name of the cluster where the event service data source is created. If you specify a cluster name, do not specify node and server names.

jdbcClassPath

The path to the JDBC driver. Specify only the path to the driver file; do not specify the file name.

dbHostName

The host name of the server where the database is installed.

dbUser

The DB2 user ID to use when creating the event database. The specified user ID must have sufficient privileges to create and drop databases.

dbPassword

The DB2 password to use.

Other parameters might be required for your environment. For a complete list of parameters and usage information, refer to the help for the **configEventServiceDB2ZOSDB** administrative command.

Results

The administrative command creates the required data source at the specified scope; if you are running the command on a Linux, UNIX, or Windows DB2 client and you specified `true` for the createDB parameter, the command also runs the generated database configuration script to create the database. On a z/OS system, you must use the SQL Processor Using File Input (SPUFI) facility to run the generated DDL files. The DDL files are stored in the *profile_root*/databases/event/*node*/*server*/db2zos/ddl directory.

The generated database configuration scripts are stored by default in the *profile_root*/databases/event/*node*/*server*/dbscripts/db2zos directory. (In a Network Deployment environment, these scripts are stored under the deployment manager profile directory.) If you specified a value for the optional outputScriptDir parameter, the scripts are stored in that location instead. You can use these scripts to manually configure the event database at any time.

What to do next

After you have finished configuring the database, you can use the server administrative console to test the database configuration. To perform this task, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Configuring a DB2 database on an iSeries system

You can configure an event database on an iSeries system using DB2 database software.

About this task

If you are using a local iSeries server to configure a remote iSeries server, you must specify a remote database entry on your local server as an alias to the target database. To configure the event database:

Procedure

1. Start the wsadmin tool.
2. Use the AdminTask object to run the **configEventServiceDB2iSeriesDB** administrative command in batch or interactive mode. The minimum required parameters of the **configEventServiceDB2iSeriesDB** command are as follows:

   createDB
   Indicates whether the administrative command creates and run the database configuration scripts. Specify `true` or `false`. If this parameter is set to `false`, the scripts are created but are not run. You must then run the database configuration scripts to complete the database configuration.

   Limitation: The administrative command can automatically run the database configuration script only on the iSeries system. If you are running the command on a client system, an error is returned.

   nodeName
   The name of the node that contains the server where the event service data source is created. If you specify a node name, you must also specify a server name. You must specify one of the following:
   - Node name and server name
   - Cluster name

   serverName
   The name of the server where the event service data source is created.

   clusterName
   The name of the cluster where the event service data source is created. If you specify a cluster name, do not specify node and server names.

   toolboxJdbcClassPath
   The path to the IBM Toolbox for Java DB2 JDBC driver. Use this parameter only if you want to use the Toolbox for Java driver instead of the native JDBC driver. Specify only the path to the driver file; do not include the file name.

   nativeJdbcClassPath
   The path to the DB2 for iSeries native JDBC driver. Use this parameter only if you want to use the native JDBC driver instead of the Toolbox for Java driver. Specify only the path to the driver file; do not include the file name.

   dbHostName
   The host name of the server where the database is installed. This parameter is required if you are using the Toolbox for Java JDBC driver.

   dbUser
   The DB2 user ID to use when creating the event database. The specified user ID must have sufficient privileges to create and drop databases.

dbPassword
> The DB2 password to use.

Other parameters might be required for your environment. For a complete list of parameters and usage information, refer to the help for the **configEventServiceDB2iSeriesDB** administrative command.

Results

The administrative command generates scripts to create the required database and data source at the specified scope. These scripts are stored by default in the *profile_root*/databases/event/*node*/*server*/dbscripts/db2iseries directory. If you specified a value for the optional outputScriptDir parameter, the scripts are stored in that location instead. You can use these scripts to manually configure the event database at any time.

What to do next

If you ran the database configuration administrative command on a client system, you must transfer the generated scripts to the iSeries system and run them to create the required resources.

After you have finished configuring the database, you can use the server administrative console to test the database configuration. To do test the configuration, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Configuring an Informix event database
You can configure an external event database using IBM Informix Dynamic Server on a Linux, UNIX, or Windows system.

About this task

To configure an Informix event database:

Procedure
1. Start the wsadmin tool.
2. Use the AdminTask object to run the **configEventServiceInformixDB** administrative command in batch or interactive mode. The minimum required parameters of the **configEventServiceInformixDB** command are as follows:

   createDB
   > Indicates whether the administrative command should create and run the database configuration scripts. Specify `true` or `false`. If this parameter is set to `false`, the scripts are created but are not run. You must then run the database configuration scripts to complete the database configuration.
   >
   > **Privileges:** If you specify `true` for this parameter, make sure your user ID has sufficient privileges for creating Informix databases, dbspaces, tables, views, indexes, and stored procedures.

   nodeName
   > The name of the node that contains the server where the event service data source should be created. If you specify a node name, you must also specify a server name. You must specify one of the following:
   > - Node name and server name
   > - Cluster name

serverName

> The name of the server where the event service data source should be created.

clusterName

> The name of the cluster where the event service data source should be created. If you specify a cluster name, do not specify node and server names.

jdbcClassPath

> The path to the JDBC driver. Specify only the path to the driver file; do not specify the file name.

dbInformixDir

> The directory where the Informix database software is installed. This parameter is required only if you specified `true` for the createDB parameter.

dbHostName

> The host name of the system where the database server is installed.

dbServerName

> The Informix server name (for example, `ol_servername`).

dbUser

> The Informix database schema user ID that will own the event database tables. This must be a user ID with sufficient privileges to create databases and dbspaces. The WebSphere data source uses this user ID to authenticate the Informix database connection.

dbPassword

> The password of the specified schema user ID.

Other parameters might be required for your environment. For a complete list of parameters and usage information, refer to the help for the **configEventServiceInformixDB** administrative command.

Results

The administrative command creates the required data source at the specified scope; if you specified `true` for the createDB parameter, the command also runs the generated database configuration script to create the database.

The generated database configuration scripts are stored by default in the *profile_root*/databases/event/*node*/*server*/dbscripts/informix directory. (In a Network Deployment environment, these scripts are stored under the deployment manager profile directory.) If you specified a value for the optional outputScriptDir parameter, the scripts are stored in that location instead. You can use these scripts to manually configure the event database at any time.

Running the scripts: The database configuration and removal scripts generated by the **configEventServiceInformixDB** administrative command require the **dbaccess** command in order to run SQL scripts. This command might be available only on the Informix server. Therefore, if the Informix server is on a different system from the server, the database configuration scripts might need to be copied to the Informix server and run locally.

Configuring an Oracle event database

You can configure an external event database using Oracle Database on a Linux, UNIX, or Windows system.

Before you begin

Before you configure an Oracle event database, you must first create the database. The Oracle SID must already exist before you run the event database configuration command. The default SID for the event database is `event`.

About this task

To configure an Oracle event database:

Procedure

1. Start the wsadmin tool.
2. Use the AdminTask object to run the **configEventServiceOracleDB** administrative command in batch or interactive mode. The minimum required parameters of the **configEventServiceOracleDB** command are as follows:

    createDB
    Indicates whether the administrative command should create and run the database configuration scripts. Specify `true` or `false`. If this parameter is set to `false`, the scripts are created but are not run. You must then run the database configuration scripts to complete the database configuration.

    nodeName
    The name of the node that contains the server where the event service data source should be created. If you specify a node name, you must also specify a server name. You must specify one of the following:

    • Node name and server name
    • Cluster name

    serverName
    The name of the server where the event service data source should be created.

    clusterName
    The name of the cluster where the event service data source should be created. If you specify a cluster name, do not specify node and server names.

    jdbcClassPath
    The path to the JDBC driver. Specify only the path to the driver file; do not specify the file name.

    oracleHome
    The ORACLE_HOME directory. This parameter is required only if you specified `true` for the createDB parameter.

    dbPassword
    The password to use for the schema user ID created during the database configuration (the default user ID is `ceiuser`. This password is used to authenticate the Oracle database connection.

    sysUser
    The Oracle SYSUSER user ID. This user ID must have SYSDBA privileges.

    sysPassword
    The password for the specified SYSUSER user ID.

    Other parameters might be required for your environment. For a complete list of parameters and usage information, refer to the help for the **configEventServiceOracleDB** administrative command.

Results

The administrative command creates the required data source at the specified scope; if you specified true for the createDB parameter, the command also runs the generated database configuration script to create the database.

The generated database configuration scripts are stored by default in the *profile_root*/databases/event/*node*/*server*/dbscripts/oracle directory. (In a Network Deployment environment, these scripts are stored under the deployment manager profile directory.) If you specified a value for the optional outputScriptDir parameter, the scripts are stored in that location instead. You can use these scripts to manually configure the event database at any time.

Configuring a SQL Server event database

You can configure an external event database using Microsoft SQL Server Enterprise on a Windows system.

About this task

To configure a SQL Server event database:

Procedure

1. On the SQL Server database server system, create the directory used to contain the database files. By default, the files are written to the c:\program files\ibm\event\ceiinst1\sqlserver_data directory. If you need to specify a different location, you must edit the generated database configuration script to modify the value of the ceiInstancePrefix parameter, and then run the script manually.

2. On the server system, start the wsadmin tool.

3. Use the AdminTask object to run the **configEventServiceSQLServerDB** administrative command in batch or interactive mode. The minimum required parameters of the **configEventServiceSQLServerDB** command are as follows:

   createDB
   Indicates whether the administrative command should create and run the database configuration scripts. Specify true or false. If this parameter is set to false, the scripts are created but are not run. You must then run the database configuration scripts to complete the database configuration.

   nodeName
   The name of the node that contains the server where the event service data source should be created. If you specify a node name, you must also specify a server name. You must specify one of the following:
   • Node name and server name
   • Cluster name

   serverName
   The name of the server where the event service data source should be created. If you specify a server name, you must also specify a node name.

   clusterName
   The name of the cluster where the event service data source should be created. If you specify a cluster name, do not specify node and server names.

dbServerName
The server name of the SQL Server database. This parameter is required only if you specified `true` for the createDB parameter.

dbHostName
The host name of the server where the SQL Server database is running.

dbPassword
The password to use for the user ID created to own the event database tables (the default user ID is ceiuser). The WebSphere data source uses this password to authenticate the SQL Server database connection.

saUser
A user ID with privileges to create and drop databases and users. This parameter is required only if you specified `true` for the createDB parameter.

saPassword
The password for the specified SA user.

Other parameters might be required for your environment. For a complete list of parameters and usage information, refer to the help for the **configEventServiceSQLServerDB** administrative command.

Results

The administrative command creates the required data source at the specified scope; if you specified `true` for the createDB parameter, the command also runs the generated database configuration script to create the database.

The generated database configuration scripts are stored by default in the *profile_root*/databases/event/*node*/*server*/dbscripts/dbscripts/sqlserver directory. (In a Network Deployment environment, these scripts are stored under the deployment manager profile directory.) If you specified a value for the optional outputScriptDir parameter, the scripts are stored in that location instead. You can use these scripts to manually configure the event database at any time.

Manually running database configuration scripts
You can manually run the scripts generated by the database configuration administrative commands at any time.

About this task

Database configuration is a two-step process. The database configuration administrative command first generates a database-specific script for your environment; this generated script then configures the event database and data sources. If you specify `true` for the createDB parameter when running the administrative command, both steps happen automatically.

However, if you specify `false` for the createDB parameter, you must complete the database configuration by manually running the generated script on the target system. You might need to run the script manually in any of the following situations:

* You need to configure the event database on a different system from the one where you ran the administrative command.
* You need to re-create the event database at a later time.
* You need to modify the default options used by the generated script before running it.

Manually creating a Derby event database:

Use the cr_event_derby command to manually generate a database configuration script for a Derby event database

About this task

To manually run the generated database configuration script for a Derby event database:

Procedure

1. On the server system, go to the directory containing the generated script. The default location is the *install_root*/profiles/*profile_name*/dbscripts/ CEI_*ceiDbName* directory; if you specified a value for the outputScriptDir parameter of the database configuration administrative command, the scripts are stored in that location instead.

2. Using an ASCII text editor, make any required modifications to the configuration script. The name of the script varies depending upon the operating system in use:

   - **Windows** cr_event_derby.bat

   - **Linux** **UNIX** cr_event_derby.sh

   - **On i5/OS platforms**: cr_event_derby

3. Optional: If you are configuring the database on an iSeries system, start the Qshell interpreter.

4. Run the database creation script using the following syntax (remember to specify the file extension, if applicable):

   ```
   cr_event_derby -p profile_path [-s server_name|-c cluster_name]
   ```

   The parameters are as follows:

   -p *profile_path*
     The path to the WebSphere profile directory. This parameter is required.

   -s *server_name*
     The name of the server. This parameter is required if you are configuring the database at the server scope.

   -c *cluster_name*
     The name of the cluster. This parameter is required if you are configuring the database at the cluster scope.

   For example, the following command would create the Derby database at the scope of the server1 server, using the profile profile1:

   ```
   cr_event_derby -p c:\WebSphere\appserver\profiles\myprofile -s server1
   ```

5. Restart the server. For a federated node, you must also stop and restart the node agent using the **stopNode** and **startNode** commands.

What to do next

After you finish configuring the database, you can use the administrative console to test the database configuration. To do this, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Manually creating a DB2 event database on a Linux, UNIX, or Windows system:

Use the cr_event_db2 to manually generate a database configuration script for a
DB2 event database on a Linux, UNIX, or Windows server.

About this task

To manually run the generated database configuration script for a DB2 event
database on a Linux, UNIX, or Windows system:

Procedure

1. On the server system, go to the directory containing the generated script. The
   default location is the *install_root*/profiles/*profile_name*/dbscripts/
   CEI_*ceiDbName* directory; if you specified a value for the outputScriptDir
   parameter of the database configuration administrative command, the scripts
   are stored in that location instead.

2. Using an ASCII text editor, make any required modifications to the
   configuration script. The name of the script varies depending upon the
   operating system in use:

   - `Windows` Windows systems: cr_event_db2.bat

   - `Linux` `UNIX` Linux and UNIX systems: cr_event_db2.sh

3. Run the database creation script using the following syntax (remember to
   specify the file extension, if applicable):

   `cr_event_db2 [client|server] db_user [db_password]`

   The parameters are as follows:

   client|server
   > Indicates whether the database is a client or server. You must specify either
   > **client** or **server**.

   db_user
   > The database user ID. This parameter is required.

   db_password
   > The password for the database user. If you do not specify a password for a
   > client database, you are prompted for it.

   For example, the following command would create the DB2 event database for
   a client database, using the user ID db2admin and the password mypassword:

   `cr_event_db2 client db2admin mypassword`

4. Restart the server. For a federated node, you must also stop and restart the
   node agent using the **stopNode** and **startNode** commands.

What to do next

After you finish configuring the database, you can use the administrative console
to test the database configuration. To do this, navigate to the appropriate JDBC
data source and select the **Test Connection** option.

Manually creating a DB2 event database on a z/OS system:

Use the cr_event_db2zos to manually generate a database configuration script for a
DB2 event database on a z/OS system, using a Linux, UNIX, or Windows client
system.

About this task

To manually run the generated database configuration script for a DB2 event database on a z/OS system, using a Linux, UNIX, or Windows client system:

Procedure
1. On the server system, go to the directory containing the generated script. The default location is the *install_root*/profiles/*profile_name*/dbscripts/ CEI_*ceiDbName* directory. If you specified a value for the outputScriptDir parameter of the database configuration administrative command, the scripts are stored in that location instead.
2. Using an ASCII text editor, make any required modifications to the configuration script. The name of the script varies depending upon the operating system in use:
   - Windows systems: cr_event_db2zos.bat
   - Linux and UNIX systems: cr_event_db2zos.sh
3. Run the database creation script using the following syntax (remember to specify the file extension, if applicable):

   cr_event_db2zos [dbName=*db_name*] *db_user* [*db_password*]

   The parameters are as follows:

   db_name
   > The database name to use. This parameter is optional; if you do not specify a database name, a name is generated.

   db_user
   > The database user ID to use. This parameter is required.

   db_password
   > The password for the database user. If you do not specify the password, the DB2 database prompts you for it.

   For example, the following command would create a DB2 event database called event, using the user ID db2admin and the password mypassword:

   cr_event_db2zos dbName=client db2admin mypassword
4. Restart the server. For a federated node, you must also stop and restart the node agent using the **stopNode** and **startNode** commands.

What to do next

After you finish configuring the database, you can use the administrative console to test the database configuration. To do this, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Manually creating a DB2 event database on an iSeries system:

Use the cr_event_db2iseries command to manually generate a database configuration script for a DB2 event database on an iSeries system

About this task

To manually run the generated database configuration script for a DB2 event database on an iSeries system:

Procedure

1. On the server system, go to the directory containing the generated script. The default location is the *install_root*/profiles/*profile_name*/dbscripts/ CEI_*ceiDbName* directory. If you specified a value for the outputScriptDir parameter of the database configuration administrative command, the scripts are stored in that location instead.

2. Using an ASCII text editor, make any required modifications to the cr_event_db2iseries script.

3. Start the Qshell interpreter.

4. Run the database creation script using the following syntax:

   cr_event_db2iseries *db_user db_password*

   The parameters are as follows:

   db_user
   The database user ID. This parameter is required.

   db_password
   The password for the database user. This parameter is required.

   For example, the following command would create the DB2 event database using the user ID db2admin and the password mypassword:

   cr_event_db2iseries db2admin mypassword

5. Restart the server. For a federated node, you must also stop and restart the node agent using the **stopNode** and **startNode** commands.

What to do next

After you finish configuring the database, you can use the administrative console to test the database configuration. To do this, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Manually creating an Informix event database:

You can manually run the scripts generated by the database configuration administrative commands at any time.

About this task

To manually run the generated database configuration scripts for an Informix event database:

Procedure

1. On the server system, go to the directory containing the generated script. The default location is the *install_root*/profiles/*profile_name*/databases/event/ SupportCluster/dbscripts/informix directory. If you specified a value for the **outputScriptDir** parameter of the database configuration administrative command, the scripts are stored in that location instead.

2. Using an ASCII text editor, make any required modifications to the configuration script. The name of the script varies depending upon the operating system in use:

   - Windows Windows systems: cr_event_informix.bat

   - Linux UNIX Linux and UNIX systems: cr_event_informix.sh

3. Run the database creation script, with no parameters.

4. Restart the server. For a federated node, you must also stop and restart the node agent using the **stopNode** and **startNode** commands.

What to do next

After you finish configuring the database, you can use the administrative console to test the database configuration. To do this, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Manually creating an Oracle event database:

Use the cr_event_oracle command to manually generate a database configuration script for an Oracle event database.

About this task

To manually run the generated database configuration script for an Oracle event database:

Procedure
1. On the server system, go to the directory containing the generated script. The default location is the*install_root*/profiles/*profile_name*/dbscripts/ CEI_*ceiDbName* directory. If you specified a value for the outputScriptDir parameter of the database configuration administrative command, the scripts are stored in that location instead.
2. Using an ASCII text editor, make any required modifications to the configuration script. The name of the script varies depending upon the operating system in use:

   - Windows Windows systems: cr_event_oracle.bat

   - Linux   UNIX Linux and UNIX systems: cr_event_oracle.sh
3. Run the database creation script using the following syntax (remember to specify the file extension, if applicable):

   ```
   cr_event_oracle password sys_user
     sys_password [sid=sid]
     [oracleHome=oracle_home]
   ```

   The parameters are as follows:

   password
   > The password for the schema user ID. This parameter is required.

   sys_user
   > The user ID that has SYSDBA privileges in the Oracle database (typically the sys user). This parameter is required.

   sys_password
   > The password for the specified sys user ID. If this user ID does not use a password, type none.

   sid=*sid*
   > The Oracle system identifier (SID). This parameter is optional.

   oracleHome=*oracle_home*
   > The Oracle home directory. This parameter is optional; if you do not specify a value, a generated path is used.

   For example, the following command would create the Oracle event database using the schema user ID auser and the sys user ID sys:

```
cr_event_oracle auser sys syspassword sid=event oracleHome=c:\oracle
```
4. Restart the server. For a federated node, you must also stop and restart the node agent using the **stopNode** and **startNode** commands.

What to do next

After you finish configuring the database, you can use the administrative console to test the database configuration. To do this, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Manually creating a SQL Server event database:

Use the cr_event_mssql command to manually generate a database configuration script for a SQL Server event database.

About this task

To manually run the generated database configuration script for a SQL Server event database:

Procedure

1. On the server system, go to the directory containing the generated script. The default location is the*install_root*/profiles/*profile_name*/dbscripts/ CEI_*ceiDbName* directory. If you specified a value for the outputScriptDir parameter of the database configuration administrative command, the scripts are stored in that location instead.
2. Using an ASCII text editor, make any required modifications to the cr_event_mssql.bat script.
3. Run the database creation script using the following syntax:
   ```
   cr_event_mssql user_id password [server=server] sauser=sa_user
    sapassword=sa_password
   ```

   The parameters are as follows:

   user_id
   > The SQL Server login user ID that will own the created tables. This user ID must be created in SQL Server so that a JDBC connection can be made to the database. (The JDBC drivers do not support trusted connections.)

   password
   > The password for the new login user ID that is created.

   server=*server*
   > The name of the server that contains the SQL Server database. This parameter is optional; the default value is the local host.

   sauser=*sa_user*
   > The sa user ID. This user ID must have sufficient privileges to create databases and user logins.

   sapassword=*sa_password*
   > The sa password, if using mixed authentication mode. If the sa user ID does not have a password set, specify sapassword= with no value. Omit this parameter if you are using a trusted connection.

   For example, the following command would create the SQL Server event database using the login user ID userid:
   ```
   cr_event_mssql userid apassword server=myserver sauser=sa sapassword=sapassword
   ```

4. Restart the server. For a federated node, you must also stop and restart the node agent using the **stopNode** and **startNode** commands.

What to do next

After you finish configuring the database, you can use the administrative console to test the database configuration. To do this, navigate to the appropriate JDBC data source and select the **Test Connection** option.

Upgrading the event database from a previous version

If you have migrated from a previous version of Common Event Infrastructure and you are using event persistence, you might need to upgrade an existing event database.

About this task

Upgrading the event database is required if you are migrating from Common Event Infrastructure version 5.1 or earlier.

The database upgrade process upgrades the schema and metadata of the existing event database to the current version while preserving existing event data.

The database upgrade script upgrades the schema and metadata of the existing event database to the current version.

Unsupported versions: If your event database uses a version of database software that is no longer supported by Common Event Infrastructure 6.0, you must first migrate the database to a supported version using the appropriate procedure for the database software. You can then follow the event database upgrade process to upgrade the database.

Upgrading a DB2 event database from a previous version:

If you have an existing DB2 event database from Version 5.1 of Common Event Infrastructure on a Linux, UNIX, or Windows system, you must upgrade it to the current version.

About this task

To upgrade a DB2 event database on a Linux or UNIX system:

Procedure
1. Make a backup copy of the existing event database.
2. Go to the *profile_root*/bin directory.
3. Run the DB2 upgrade script for your operating system:
   - `Windows` Windows systems:

     ```
     eventUpgradeDB2 runUpgrade=[true|false] dbUser=user
       [dbName=name] [dbPassword=pw]
       [dbNode=node] [scriptDir=dir]
     ```

   - `Linux` `UNIX` Linux and UNIX systems:

     ```
     eventUpgradeDB2.sh runUpgrade=[true|false] dbUser=user
       [dbName=name] [dbPassword=pw]
       [dbNode=node] [scriptDir=dir]
     ```

   The typical required parameters are as follows:

runUpgrade

Indicates whether you want the upgrade script to automatically run the generated DDL scripts to complete the database upgrade. This parameter is required. Specify `false` if you want to manually perform the database upgrade at a later time or on a different system.

dbUser

Specifies the DB2 user ID to use. This parameter is required.

dbName

Specifies the DB2 database name. The default name for the event database is `event`. This parameter is required if you specified `runUpgrade=true`.

dbPassword

Specifies the password for the specified DB2 user ID. This parameter is optional; if you do not specify a password, DB2 prompts you to type it.

dbNode

Specifies the database node name. This parameter is required if you are running the upgrade script from a DB2 client system.

scriptDir

Specifies the directory you want to contain the generated DDL scripts. This parameter is optional; if you do not specify a directory, the scripts are stored in the .\eventDBUpgrade\db2 directory.

To see a complete list of parameters and usage information, run the **eventUpgradeDB2** script with no parameters.

Results

The upgrade script generates the required DDL scripts for upgrading the event database. If you specified `runUpgrade=true`, the DDL scripts are automatically run, completing the upgrade.

Example

The following example upgrades an existing DB2 database on a Windows system:
```
eventUpgradeDB2 runUpgrade=true dbUser=db2inst1 dbName=event
```

What to do next

If you specified `runUpgrade=false`, you must manually run the DDL scripts on the database system to complete the database upgrade.

Upgrading a DB2 for z/OS event database from a previous version:

If you have an existing DB2 event database from Version 5.1 of Common Event Infrastructure on a z/OS system, you must upgrade it to the current version.

About this task

To upgrade a DB2 event database on a z/OS system:

Procedure
1. Make a backup copy of the existing event database.
2. Go to the *profile_root*/bin directory.
3. Run the DB2 for z/OS upgrade script for your client operating system:

- `Windows` Windows systems:

```
eventUpgradeDB2ZOS runUpgrade=[true|false] dbUser=user
  [dbName=name] [dbPassword=pw]
  [scriptDir=dir] storageGroup=group
  bufferPool4K=4kbufpool bufferPool8k=8kbufpool
  bufferPool16K=16kbufpool
```

- `Linux` `UNIX` Linux and UNIX systems:

```
eventUpgradeDB2ZOS.sh runUpgrade=[true|false] dbUser=user
  [dbName=name] [dbPassword=pw]
  [scriptDir=dir] storageGroup=group
  bufferPool4K=4kbufpool bufferPool8k=8kbufpool
  bufferPool16K=16kbufpool
```

The typical required parameters are as follows:

runUpgrade
Indicates whether you want the upgrade script to automatically run the generated DDL scripts to complete the database upgrade. This parameter is required. Specify false if you want to manually upgrade the database at a later time or on a different system.

z/OS systems: This parameter is ignored on a native z/OS system. Automatically running the generated DDL scripts is supported only on a client system.

dbUser
Specifies the DB2 user ID to use. This parameter is required.

dbName
Specifies the DB2 database name. The default name for the event database is `event`. This parameter is required if you specified `runUpgrade=true`.

dbPassword
Specifies the password for the specified DB2 user ID. This parameter is optional; if you do not specify a password, DB2 prompts you to type it.

scriptDir
Specifies the directory you want to contain the generated DDL scripts. This parameter is optional; if you do not specify a directory, the scripts are stored in the .\eventDBUpgrade\db2zos directory.

storageGroup
Specifies the name of the storage group. This parameter is required.

bufferPool4K
Specifies the name of the 4K buffer pool. This parameter is required.

bufferPool8K
Specifies the name of the 8K buffer pool. This parameter is required.

bufferPool16K
Specifies the name of the 16K buffer pool. This parameter is required.

To see a complete list of parameters and usage information, run the **eventUpgradeDB2ZOS** script with no parameters.

Results

The upgrade script generates the required DDL scripts for upgrading the event database. If you specified `runUpgrade=true` on a client system, the DDL scripts are automatically run, completing the upgrade.

Example

The following example upgrades a DB2 for z/OS event database from a Windows
client system:

```
eventUpgradeDB2ZOS runUpgrade=true dbUser=db2inst1 dbName=event
  storageGroup=sysdeflt bufferPool4K=BP9 bufferPool8K=BP8K9 bufferPool16K=BP16K9
```

What to do next

If you specified `runUpgrade=false`, or if you ran the upgrade script on the z/OS
system, you must manually run the generated DDL scripts on the z/OS system
using the SQL Processor Using File Input (SPUFI) facility. This step completes the
database upgrade.

Upgrading an Oracle event database from Version 5:

If you have an existing Oracle event database from Version 5.1 of Common Event
Infrastructure, you must upgrade it to the current version.

About this task

To upgrade an Oracle event database:

Procedure
1. Make a backup copy of the existing event database.
2. Go to the *profile_root*/bin directory.
3. Run the Oracle upgrade script for your operating system:
   - Windows systems:
     ```
     eventUpgradeOracle runUpgrade=[true|false] schemaUser=schemauser
       [oracleHome=dir] [dbName=name]
       [dbUser=sysuser] [dbPassword=pw]
       [scriptDir=dir]
     ```
   - Linux and UNIX systems:
     ```
     eventUpgradeOracle.sh runUpgrade=[true|false] schemaUser=schemauser
       [oracleHome=dir] [dbName=name]
       [dbUser=sysuser] [dbPassword=pw]
       [scriptDir=dir]
     ```
   The typical required parameters are as follows:

   runUpgrade
   Indicates whether you want the upgrade script to automatically run the
   generated DDL scripts to complete the database upgrade. This parameter is
   required. Specify `false` if you want to manually upgrade the database at a
   later time or on a different system.

   schemaUser
   Specifies the Oracle user ID that owns the database tables. This parameter
   is required.

   oracleHome
   Specifies the Oracle home directory. This parameter is required if you
   specified `runUpgrade=true`.

   dbName
   Specifies the Oracle database name. The default name for the event
   database is `event`. This parameter is required if you specified
   `runUpgrade=true`.

dbUser

Specifies the Oracle sys user ID. This parameter is required if you specified `runUpgrade=true`.

dbPassword

Specifies the password for the sys user ID. Do not specify this parameter if the sys user ID has no password.

scriptDir

Specifies the directory you want to contain the generated DDL scripts. This parameter is optional; if you do not specify a directory, the scripts are stored in the .\eventDBUpgrade\oracle directory.

To see a complete list of parameters and usage information, run the **eventUpgradeOracle** script with no parameters.

Results

The upgrade script generates the required DDL scripts for upgrading the event database. If you specified `runUpgrade=true`, the DDL scripts are automatically run, completing the upgrade.

Example

The following example upgrades an existing Oracle database on a Windows system:

```
eventUpgradeOracle runUpgrade=true schemaUser=cei
  dbName=event dbUser=sys
```

What to do next

If you specified `runUpgrade=false`, you must manually run the DDL scripts on the database system to complete the database upgrade.

Configuring WebSphere Business Integration Adapters

You must perform installation and configuration procedures for the WebSphere Business Integration Adapter to work with WebSphere Process Server.

Procedure

1. Install the adapter.
   a. Follow the procedures outlined at Installing WebSphere Business Integration Adapters products, which describe how to install WebSphere Business Integration Adapters.
   b. Determine whether there are any additional required procedures that are specific to your adapter by going to the WebSphere Business Integration Adapters documentation and expanding the navigation under **Adapters**. If any additional installation tasks are listed for your adapter, perform those tasks.
2. Configure your adapter by going to the WebSphere Business Integration Adapters documentation, expanding the navigation under **Adapters**, and following the configuration instructions for your adapter. The configuration procedure generates the required artifacts.
3. Install the application EAR file by following the instructions for Deploying a mediation module.

Setting up administration of WebSphere Business Integration Adapters

You must perform several administrative functions before you can manage a WebSphere Business Integration Adapter.

Before you begin

- You must be familiar with the procedures outlined in Installing WebSphere Business Integration Adapters products.
- You must have installed the application EAR file to create the artifacts required for the WebSphere Business Integration Adapter before you perform this task.

About this task

In order to have administrative control over a WebSphere Business Integration Adapter, perform the following administrative functions.

Procedure

1. Create a Queue Connection Factory.

   From the top level of the administrative console, follow these steps:

   a. Expand **Resources**.

   b. Expand **JMS**.

   c. Select **Queue connection factories**.

   d. Select the scope level that matches the scope level of the Administration Input/Output Queues.

   e. Click **New** to create a new JMS queue connection factory.

   f. Choose the JMS resource provider. Select **Default messaging provider**, and click **OK**.

   g. Accept all the default values with the following exceptions:
      - **Name**: QueueCF
      - **JNDI Name**: jms/QueueCF
      - **BusName**: *Your bus name*

   h. Complete the creation of your new JMS queue connection factory by clicking **OK**.

      A message window appears at the top of the JMS queue connection factory panel.

   i. Apply the changes that you have made at the local configuration level to the master configuration by clicking **Save** in the message window.

2. Create a WebSphere Business Integration Adapter resource.

   From the top level of the administrative console, follow these steps:

   a. Expand **Resources**.

   b. Open the WebSphere Business Integration Adapters page.

      Select **WebSphere Business Integration Adapters**.

   c. Create a new WebSphere Business Integration Adapter by clicking **New**.

   d. Accept all the default values with the following exceptions:
      - **Name**: EISConnector
      - **Queue connection factory JNDI name**: jms/QueueCF
      - **Administration input queue JNDI name**: *connectorName/AdminInQueue*

- **Administration output queue JNDI name**: *connectorName/ AdminOutQueue*

   e. Complete the creation of the WebSphere Business Integration Adapter by clicking **OK**.

      A message window appears at the top of the WebSphere Business Integration Adapters panel.

   f. Apply the changes that you have made at the local configuration level to the master configuration by clicking **Save** in the message window.

3. Enable the WebSphere Business Integration Adapter Service.

   From the top level of the administrative console, follow these steps:

   a. Expand **Servers**.

   b. Expand **Server types**.

   c. Select **WebSphere application servers**.

   d. From the list of servers, select a server where the WebSphere Business Integration Adapter Service is to be enabled.

      Click the name of the server that hosts the resources of interest.

   e. From the **Business Integration** list on the Configuration tab, select **WebSphere Business Integration Adapter Service**.

   f. Ensure that the **Enable service at server startup** check box is selected.

   g. Click **OK**.

      A message window appears at the top of the WebSphere Business Integration Adapters page.

   h. Repeat steps 3d to 3g for each server on which the WebSphere Business Integration Adapter Service is to be enabled.

   i. Apply the changes that you have made at the local configuration level to the master configuration by clicking **Save** in the message window.

   Note: When you enable or disable a WebSphere Business Integration Adapter service, you must restart the server in order for the changes to take effect.

Configuring WebSphere Process Server for Service Federation Management

You can enable a WebSphere Process Server as a connectivity server that can be administered by the Service Federation Management (SFM) console provided with WebSphere Service Registry and Repository version 7.0. The SFM console can then configure SFM proxies in WebSphere Process Server.

About this task

You might have separate enterprise service buses (ESBs) in different business units. Each ESB and associated service registry constitute a separate domain of connected service applications. This can result in expensive duplication of applications between domains and also in increased development effort to implement application connectivity across domains. SFM, provided in WebSphere Service Registry and Repository version 7.0, allows you to establish bridges between separate ESBs, allowing services and applications to be shared between domains.

SFM provides:

- A federation model which provides a unifying view of federation relevant content.

- A Service Connectivity Management Protocol, which accesses the service connectivity and registry components supporting a domain.
- A console for controlling service domains.

SFM allows the console user to configure services in one domain so that they are available to service consumers in another domain; the service endpoints in one domain are available as service proxy endpoints in another domain.

Configuring the Service Connectivity Management connectivity server

The Service Federation Management (SFM) console uses the Service Connectivity Management Protocol (SCMP) to communicate with WebSphere Process Server.

About this task

WebSphere Process Server exposes the Atom based protocol as a system REST service named SCM Connectivity Server. This service is enabled by default in the REST service provider for stand-alone servers and the deployment manager of a Network Deployment environment.

Procedure

1. Configure the REST services. The Atom documents returned by the protocol contain absolute URLs which are retained by the SFM console. The protocol, host name, and port number used in those absolute URLs are taken from the REST service configuration. It is important to consider any load balancing and network components between the SFM console server and WebSphere Process Server.

   a. Configure the protocol, fully-qualified host name, and port number, for the stand-alone server or deployment manager REST service provider as described in the Configuring REST services in a service provider topic.

2. Provide the SFM console user with details to access the connectivity server.

   a. The URL of the Atom service document for the connectivity server can be found on the REST services panel. The service has the type *SCM Connectivity Server*.

   b. If WebSphere Process Server administrative security is enabled, the SFM console user will also require a username and password to access the service endpoint. These credentials must be for a user in the RestServicesUser group who has sufficient administrative rights to install Service Connectivity Architecture modules.

Configuring the Service Connectivity Management connectivity provider

You can configure all Service Connectivity Management (SCM) connectivity providers for your environment by using the administrative console.

About this task

An SCM connectivity provider is a logical partition of the ESB that is exposed via the SCM Protocol. It defines the target (server or cluster) to which proxy gateway modules will be deployed when a SCM group proxy is created on that connectivity provider. It also defines properties that will be used for proxy targets created on those group proxies.

Procedure

Select **Service integration > SCM connectivity providers**. The SCM connectivity providers page opens, displaying all connectivity providers in your environment.

Results

SCM connectivity providers can be added, removed, or worked with from this page.

Adding a connectivity provider

You can add a server or a cluster as a Service Connectivity Management (SCM) connectivity provider using the administrative console.

Procedure

1. Click **Service integration > SCM connectivity providers**. The SCM connectivity providers page opens, displaying all connectivity providers in your environment.
2. Click **Add** to add a server or a cluster as a connectivity provider. The wizard for adding connectivity providers will open.
3. Complete **Step 1. Select a server or cluster** on the wizard to identify the server or cluster to which SCM group proxies for this connectivity provider should be deployed. Click **Next**.
4. Complete **Step 2. Specify SCM connectivity provider properties** on the wizard to specify the properties:

Option	Description
Name	The name of the SCM connectivity provider. This must be unique within the cell. An exception is thrown if the name already exists. The name, description, contact, organization and location will be visible to users of the Service Federation Management console.
Description	A brief description of the SCM connectivity provider. This is optional and defaults to an empty string. The name, description, contact, organization and location will be visible to users of the Service Federation Management console.
Contact	The name of a contact person for the SCM connectivity provider. This is optional and defaults to an empty string. The name, description, contact, organization and location will be visible to users of the Service Federation Management console.
Organization	The name of the owning organization for the SCM connectivity provider. This is optional and defaults to an empty string. The name, description, contact, organization and location will be visible to users of the Service Federation Management console.

Option	Description
Location	The location for the SCM connectivity provider. This is optional and defaults to an empty string. The name, description, contact, organization and location will be visible to users of the Service Federation Management console.
HTTP host	The host name that will be returned for the endpoint of an insecure proxy target. This should be the host that web service clients in another domain will use to access the proxy, taking in to account web servers and other network components.
HTTP port	The port that will be returned for the endpoint of an insecure proxy target. This should be the port that web service clients in another domain will use to access the proxy, taking in to account web servers and other network components.
HTTPS host	The host name that will be returned for the endpoint of a secure proxy target. This should be the host that web service clients in another domain will use to access the proxy, taking in to account web servers and other network components.
HTTPS port	The port that will be returned for the endpoint of a secure proxy target. This should be the port that web service clients in another domain will use to access the proxy, taking in to account web servers and other network components.
Authentication Alias	The name of the authentication alias that will provide the basic authentication credentials used to retrieve WSDL documents via HTTP from the service registry associated with the SCM connectivity provider's domain. This parameter need not be specified if basic authentication is not required to connect to the service registry.
SSL configuration	The name of the SSL configuration used to retrieve WSDL documents via HTTP from a secure service registry associated with the SCM connectivity provider's domain. This is optional and, if not specified, the server's default SSL configuration will be used.

5. Click **Finish**. The SCM connectivity provider page will open, with the new connectivity provider listed.
6. Review the **Messages** section to ensure that the connectivity provider and its properties are complete.
7. Click **Save** to save the connectivity provider to the master configuration.

Removing a connectivity provider

You can remove a server or a cluster as a Service Connectivity Management (SCM) connectivity provider using the administrative console.

Procedure

1. Click **Service integration > SCM connectivity providers**. The SCM connectivity providers page opens, displaying all connectivity providers in your environment.

2. Select the connectivity provider. Click **Remove** to remove the server or cluster as a connectivity provider.

Working with connectivity providers

You can list, show, and modify a Service Connectivity Management (SCM) connectivity provider using the administrative console.

Procedure

1. Click **Service integration > SCM connectivity providers**. The SCM connectivity providers page opens, displaying all connectivity providers in your environment.

2. Select a connectivity provider to display its details page.

3. Fields can be modified on this page, although you cannot modify the **Name**, **Author**, **Created**, or **Updated** fields.

4. Use the **Apply**, **OK**, **Reset**, and **Cancel** buttons in order to complete any modifications.

Service Connectivity Management usage of Service Component Architecture modules

A Service Component Architecture module is installed every time the Service Federation Management console creates a group proxy. These Service Component Architecture modules can be viewed on the enterprise application view and Service Component Architecture module list on the administration console.

A versioned Service Component Architecture module is used for the group proxy. The base module name is ScmGroupProxy and the version number is v1_0_0. The cell identifier is formed from the connectivity provider name and a unique identifier for the group proxy within the cell.

The name of the service module as it appears in the module list is ScmGroupProxy (*ConnectivityProviderName_UniqueId*), and the service application name is of the form ScmGroupProxy_v1_0_0_*ConnectivityProviderName_UniqueID*App. The same unique identifier also forms part of the URL and Atom identifier used to access the group proxy via the SCM protocol.

A group proxy created on the connectivity provider *ExampleConnectivityProvider* with the generated unique identifier *xot5*, would result in a module with the name ScmGroupProxy (ExampleConnectivityProvider_xot5) being deployed as the application ScmGroupProxy_v1_0_0_ExampleConnectivityProvider_xot5App to the server or cluster associated with the connectivity provider.

The URL to access the Atom document representing the group proxy resource would be of the form:

```
/rest/scmp/connectivity-provider/ExampleConnectivityProvider-g0jk9fzm/
mediation/group-proxy-type/group-proxy/xot5-g0jkjal9
```

The Atom identifier for that document would be of the form:

```
urn:wesb-scmp:cell/localhostNode01Cell/connectivity-provider/
ExampleConnectivityProvider-g0jk9fzm/mediation/group-proxy-type/group-
proxy/xot5-g0jkjal9
```

Note: Attributes of the SCM group proxy appear as promoted properties of the module. These can be viewed via the administration console but must not be modified.

Service Connectivity Management mapping to proxy gateways

A Service Connectivity Management (SCM) group proxy module is implemented as a proxy gateway within WebSphere Process Server

The SCM proxy targets for the group proxy appear as virtual services of the proxy gateway and can be viewed in Business Space powered by WebSphere via the Proxy gateway widget. Properties of the proxy target appear as properties of the virtual service.

Note: Virtual services associated with SCM group proxy modules must not be added, removed, or modified, via the Proxy gateway widget.

Troubleshooting configuration

You can diagnose problems when the configuration of WebSphere Process Server is unsuccessful.

About this task

For more information about troubleshooting various errors during the product installation and configuration, see "Troubleshooting installation and configuration" on page 141.

IBM®

Printed in USA